Edge-corE

Powered by Accton

ES4626/ES4650

Layer 3 Gigabit Switch

Management Guide

www.edge-core.com

Preface

ES4626/ES4650 is a routing switch that can be deployed as the core layer device for campus and enterprise networks, or as an aggregation device for IP metropolitan area networks (MAN). The ES4626 provides 24 fixed 1000MB port (4 of which are fixed 1000MB Combo fiber cable port/copper cable ports) and 2 10GB XFP ports. The ES4650 provides 48 fixed 1000MB port (4 of which are fixed 1000MB Combo fiber cable port/copper cable ports) and 2 10GB XFP ports. ES4626/ES4650 can seamlessly support various network interfaces from 100Mb, 1000Mb to 10Gb Ethernets.

We are providing this manual for your better understanding, usage and maintenance of the ES4626/ES4650. We strongly recommend you to read through this manual carefully before the installation and configuration to avoid possible damage and malfunction to the switch. Thank you for your choice and purchase of this networking product from Accton Technology Corp. We sincerely hope our products and services satisfy you.

Contents

Preface 2

Contents 3

Chapter 1 Switch Management 12

1.1 Management Options 12

1.1.1 Out-of-band Management 12

1.1.2 In-band Management 15

1.2 Management Interface 21

1.2.1 CLI Interface 21

1.2.2 WEB Interface 28

Chapter 2 Basic Switch Configuration 30

2.1 Basic Switch Configuration Commands 30

2.1.1 calendar set 30

2.1.2 config 30

2.1.3 enable 31

2.1.4 disable 31

2.1.5 enable password 31

2.1.6 exec timeout 32

2.1.7 exit 33

2.1.8 help 33

2.1.9 ip host 33

2.1.10 hostname 34

2.1.11 uername password 34

2.1.12 uername nopassword 35

2.1.13 username access-level 35

2.1.14 reload 35

2.1.15 set default 36

2.1.16 setup 36

2.1.17 language 36

2.1.18 write 36

2.2 Maintenance and Debug Commands 37

2.2.1 ping 37

2.2.2 Telnet 38

2.2.3 SSH 41

2.2.4 traceroute 46
2.2.5 show 47
2.2.6 debug 53
2.3 Configuring Switch IP Addresses 53
2.3.1 Configuring Switch IP Addresses Task Sequence 53
2.3.2 Commands for Configuring Switch IP Addresses 54
2.4 SNMP 56
2.4.1 Introduction to SNMP 56
2.4.2 Introduction to MIB 57
2.4.3 Introduction to RMON 58
2.4.4 SNMP Configuration 59
2.4.5 Typical SNMP Configuration Examples 66
2.4.6 SNMP Troubleshooting Help 67
2.5 Switch Upgrade 72
2.5.1 BootROM Upgrade 72
2.5.2 FTP/TFTP Upgrade 75
2.6 WEB Management 90
2.6.1 Switch Basic Configuration 90
2.6.2 SNMP Configuration 91
2.6.3 Switch Upgrade 93
2.6.4 Monitor and debug command 95
2.6.5 Switch basic information 97
2.6.6 Switch on-off configuration 98
2.6.7 Switch maintenance 98
2.6.8 Telnet service configuration 99
2.6.9 username service 99
2.6.10 Basic host configuration 100
Chapter 3 Port Configuration 101
3.1 Introduction to Port 101
3.2 Port Configuration 101
3.2.1 Network Port Configuration 101
3.2.2 VLAN Interface Configuration 109
3.2.3 Port Mirroring Configuration 112
3.3 Port Configuration Example 114
3.4 Port Troubleshooting Help 115

3.4.1 Monitor and Debug Commands 115
3.4.2 Port Troubleshooting Help 116
3.5 WEB Management 116
3.5.1 Ethenet port configuration 116
3.5.2 Vlan interface configuration 118
3.5.3 Port mirroring configuration 120
3.5.4 Port debug and maintenance 120
Chapter 4 MAC Table Configuration 123
4.1 Introduction to MAC Table 123
4.1.1 Obtaining MAC Table 123
4.1.2 Forward or Filter 125
4.2 MAC Table Configuration 126
4.2.1 mac-address-table aging-time 126
4.2.2 mac-address-table static 126
4.2.3 mac-address-table discard 127
4.3 Typical Configuration Examples 128
4.4 Troubleshooting Help 128
4.4.1 Monitor and Debug Commands 128
4.4.2 Troubleshooting Help 129
4.5 MAC Address Function Extension 129
4.5.1 MAC Address Binding 129
4.6 WEB Management 137
4.6.1 MAC address table configuration 137
4.6.2 MAC address table configuration 140
Chapter 5 VLAN Configuration 145
5.1 Introduction to VLAN 145
5.2 VLAN Configuration 146
5.2.1 VLAN Configuration Task Sequence 146
5.2.2 VLAN Configuration Commands 148
5.2.3 Typical VLAN Application 152
5.3 GVRP Configuration 154
5.3.1 GVRP Configuration Task Sequence 155
5.3.2 GVRP Commands 156
5.3.3 Typical GVRP Application 158

5.4 VLAN Troubleshooting Help 160
5.4.1 Monitor and Debug Information 160
5.4.2 VLAN Troubleshooting Help 162
5.5 WEB Management 162
5.5.1 Vlan configuration 162
5.5.2 GVRP configuration 168
5.5.3 VLAN debug and maintenance 169
Chapter 6 MSTP Configuration 171
6.1 MSTP Introduction 171
6.1.1 MSTP Region 171
6.1.2 Port Roles 173
6.1.3 MSTP Load Balance 173
6.2 Configuring MSTP 173
6.2.1 MSTP Configuration Task Sequence 173
6.2.2 MSTP Configuration Command 176
6.3 MSTP Example 184
6.4 MSTP Troubleshooting 189
6.4.1 Monitoring And Debugging Command 189
6.4.2 MSTP Troubleshooting Help 193
Chapter 7 IGMP Snooping Configuration 194
7.1 Introduction to IGMP Snooping 194
7.2 IGMP Snooping Configuration 194
7.2.1 IGMP Snooping Configuration Task 194
7.2.2 IGMP Snooping Configuration Command 196
7.3 IGMP Snooping Example 199
7.4 IGMP Snooping Troubleshooting Help 202
7.4.1 Monitor and Debug Commands 202
7.4.2 IGMP Snooping Troubleshooting Help 206
7.5 Web Management 206
7.5.1 Enable IGMP Snooping on the switch 206
7.5.2 IGMP Snooping Configuration 206
7.5.3 IGMP Snooping static multicast configuration 208
Chapter 8 802.1X CONFIGURATION 210
8.1 802.1X Introduction 210

8.2 802.1X Configuration 211
8.2.1 802.1X Configuration Task Sequence 211
8.2.2 802.1X Configuration Command 216
8.3 802.1X Apply Example 226
8.4 802.1X Trouble Shooting 227
8.4.1 802.1X Debug and Monitor Command 227
8.4.2 802.1X Troubleshooting 232
8.5 WEB Management 233
8.5.1 RADIUS client configuration 233
8.5.2 802.1X Configuration 235
Chapter 9 ACL Configuration 239
9.1 Introduction to ACL 239
9.1.1 Access list 239
9.1.2 Access-group 239
9.1.3 Access list Action and Global Default Action 240
9.2 ACL configuration 240
9.2.1 ACL Configuration Task Sequence 240
9.2.2 ACL Configuration Commands 244
9.3 ACL Example 249
9.4 ACL Troubleshooting Help 250
9.4.1 ACL Debug and Monitor Commands 250
9.4.2 ACL Troubleshooting Help 252
9.5 Web Management 252
9.5.1 Add standard numeric IP ACL configuration 253
9.5.2 Delete standard numeric IP ACL configuration 253
9.5.3 Extended numeric ACL configuration 253
9.5.4 Standard ACL name configuration 255
9.5.5 Extended ACL name configuration 256
9.5.6 Firewall configuration 256
9.5.7 ACL port binding configuration 257
Chapter 10 Port Channel Configuration 258
10.1 Introduction to Port Channel 258
10.2 Port Channel Configuration 259
10.2.1 Port Channel Configuration Task Sequence 259
10.2.2 Port Channel Configuration Commands 260

10.3 Port Channel Example 262
10.4 Port Channel Troubleshooting Help 264
10.4.1 Monitor and Debug Commands 264
10.4.2 Port Channel Troubleshooting Help 269
10.5 Web Management 270
10.5.1 LACP port group configuration 270
10.5.2 LACP port configuration 271
Chapter 11 DHCP Configuration 272
11.1 Introduction to DHCP 272
11.2 DHCP Server Configuration 273
11.2.1 DHCP Sever Configuration Task Sequence 273
11.2.2 DHCP Server Configuration Commands 275
11.3 DHCP Relay Configuration 284
11.3.1 DHCP Relay Configuration Task Sequence 285
11.3.2 DHCP Relay Configuration Command 285
11.4 DHCP Configuration Example 287
11.5 DHCP Troubleshooting Help 289
11.5.1 Monitor and Debug Commands 289
11.5.2 DHCP Troubleshooting Help 294
11.6 WEB Management 294
11.6.1 DHCP server configuration 294
11.6.2 DHCP relay configuration 301
11.6.3 DHCP debugging 302
Chapter 12 SNTP Configuration 304
12.1 SNTP Configuration Commands 304
12.1.1 sntp server 304
12.1.2 sntp poll 304
12.1.3 clock timezone 305
12.2 Typical SNTP Configuration Examples 306
12.3 SNTP Troubleshooting Help 306
12.3.1 Monitor and Debug Commands 306
12.4 WEB Management 307
12.4.1 SNTP/NTP server configuration 307
12.4.2 Request interval configuration 307

12.4.3 Time difference 308
12.4.4 Show sntp 308
Chapter 13 QoS Configuration 309
13.1 QoS 309
13.1.1 Introduction to QoS 309
13.1.2 QoS Configuration 311
13.1.3 QoS Example 325
13.1.4 QoS Troubleshooting Help 327
13.1.5 Web Management 333
13.2 PBR 345
13.2.1 PBR Introduction 345
13.2.2 PBR Configuration 345
13.2.3 PBR Example 349
Chapter 14 L3 Forward Configuration 351
14.1 Layer3 Interface 351
14.1.1 Introduction to Layer3 Interface 351
14.1.2 Layer3 interface configuration 352
14.2 IP Forwarding 353
14.2.1 Introduction to IP Forwarding 353
14.2.2 IP Route Aggregation Configuration 353
14.2.3 IP Forwarding Troubleshooting Help 354
14.3 ARP 356
14.3.1 Introduction to ARP 356
14.3.2 ARP configuration 357
14.3.3 ARP Forwarding Troubleshooting Help 358
Chapter 15 Routing Protocol Configuration 361
15.1 Route Table 361
15.2 Static Route 362
15.2.1 Introduction to Static Route 362
15.2.2 Introduction to Default Route 363
15.2.3 Static Route Configuration 363
15.2.4 Configuration Scenario 366
15.2.5 Troubleshooting Help 367
15.3 RIP 367
15.3.1 Introduction to RIP 367

15.3.2 RIP Configuration 369
15.3.3 Typical RIP Scenario 385
15.3.4 RIP Troubleshooting Help 387
15.4 OSPF 389
15.4.1 Introduction to OSPF 389
15.4.2 OSPF Configuration 392
15.4.3 Typical OSPF Scenario 417
15.4.4 OSPF Troubleshooting Help 424
15.5 Web Management 433
15.5.1 Static route 433
15.5.2 RIP 434
15.5.3 OSPF 438
Chapter 16 Multicast Protocol Configuration 447
16.1 Multicast Protocol Overview 447
16.1.1 Introduction to Multicast 447
16.1.2 Multicast Address 448
16.1.3 IP Multicast Packets Forwarding 449
16.1.4 Application of Multicast 449
16.2 Common Multicast Configurations 450
16.2.1 Common Multicast Configuration Commands 450
16.3 PIM-DM 451
16.3.1 Introduction to PIM-DM 451
16.3.2 PIM-DM Configuration 452
16.3.3 Typical PIM-DM Scenario 454
16.3.4 PIM-DM Troubleshooting Help 455
16.4 PIM-SM 459
16.4.1 Introduction to PIM-SM 459
16.4.2 PIM-SM Configuration 460
16.4.3 Typical PIM-SM Scenario 465
16.4.4 PIM-SM Troubleshooting Help 467
16.5 DVMRP 472
16.5.1 Introduction to DVMRP 472
16.5.2 DVMRP configuration 473
16.5.3 Typical DVMRP Scenario 480
16.5.4 DVMRP Troubleshooting Help 480

16.6 IGMP 485
16.6.1 Introduction to IGMP 485
16.6.2 IGMP configuration 486
16.6.3 Typical IGMP Scenario 492
16.6.4 IGMP Troubleshooting Help 492
16.7 web Management 495
16.7.1 Multicast common configuration 495
16.7.2 PIM-DM configuration 496
16.7.3 PIM-SM configuration 496
16.7.4 DVMRP configuration 498
16.7.5 IGMP configuration 500
16.7.6 Multicast inspect and debug 501
Chapter 17 VRRP Configuration 503
17.1 Introduction to VRRP 503
17.2 VRRP Configuration 504
17.2.1 VRRP Configuration Task Sequence 504
17.2.2 VRRP Configuration Commands 505
17.2.3 Typical VRRP Application 510
17.2.4 VRRP Troubleshooting Help 511
Chapter 18 Cluster Network Management 514
18.1 Introduction to cluster network management 514
18.2 Basic Cluster Network Management Configuration 515
18.2.1 Cluster Network Management Configuration Sequence 515
18.2.2 Cluster Configuration Commands 517

Chapter 1 Switch Management

1.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. ES4626/ES4650 provides two management options: in-band management and out-of-band management.

1.1.1 Out-of-band Management

Out-of-band management is the management through Console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available. For instance, the user must assign an IP address to the switch via the Console interface to be able to access the switch through Telnet.

The procedures for managing the switch via Console interface are listed below:

Step 1: setting up the environment:

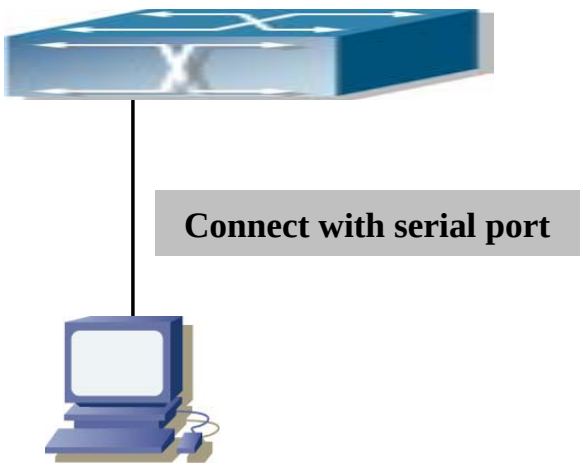


Fig 1-1 Out-of-band Management Configuration Environment

As shown in Fig 1-1, the serial port (RS-232) is connected to the switch with the serial cable provided. The table below lists all the devices used in the connection.

Device Name	Description
PC machine	Has functional keyboard and RS-232, with terminal emulator installed, such as HyperTerminal included in Windows 9x/NT/2000/XP.

Serial port cable	One end attach to the RS-232 serial port, the other end to the Console port.
ES4626/ES4650	Functional Console port required.

Step 2 Entering the HyperTerminal

Open the HyperTerminal included in Windows after the connection established. The example below is based on the HyperTerminal included in Windows XP.

1) Click Start menu - All Programs – Accessories – Communication - HyperTerminal.

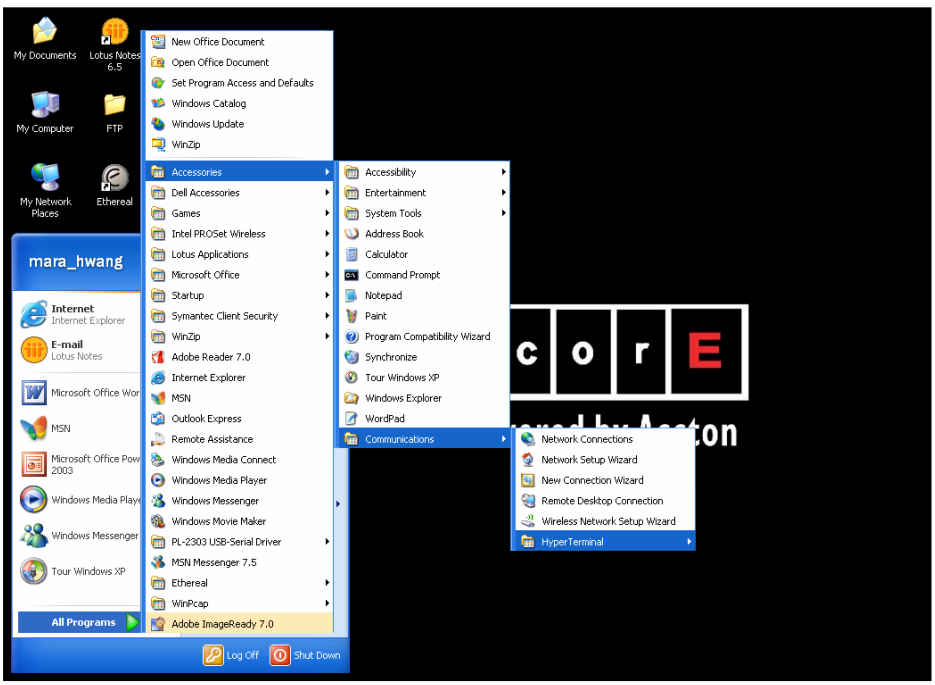


Fig 1-2 Opening HyperTerminal (1)

2) Type a name for opening HyperTerminal, such as “Switch”.

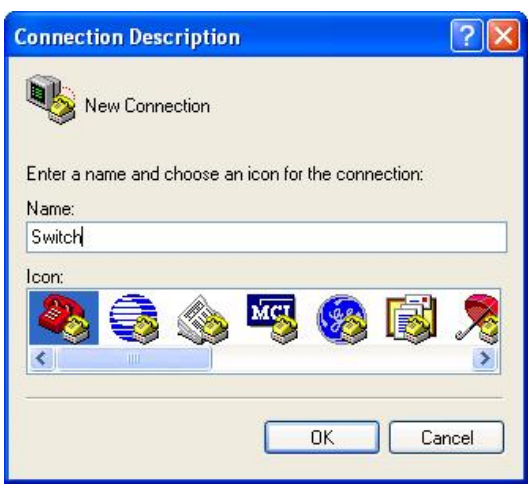


Fig 1-3 Opening HyperTerminal (2)

3) In the “Connecting with” drop-list, select the RS-232 serial port used by the PC, e.g. COM1, and click “OK”.

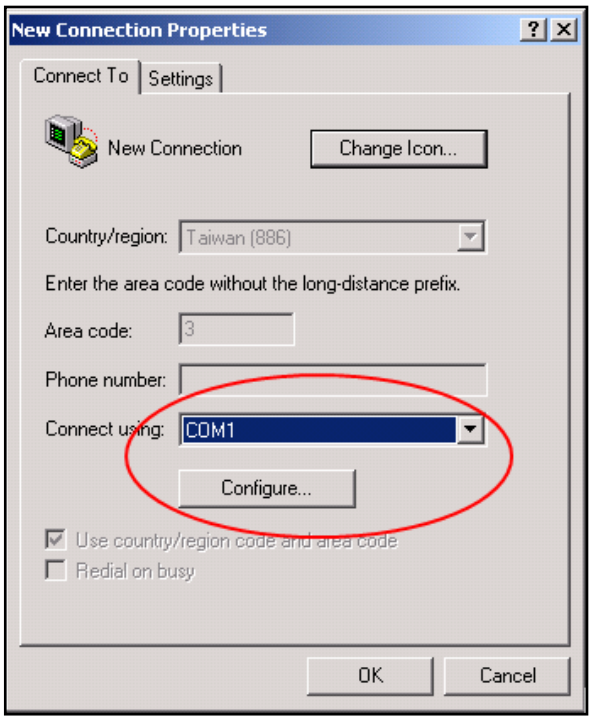


Fig 1-4 Opening HyperTerminal (3)

4) COM1 property appears, select “9600” for “Baud rate”, “8” for “Data bits”, “none” for “Parity checksum”, “1” for stop bit and “none” for traffic control; or, you can also click “Revert to default” and click “OK”.

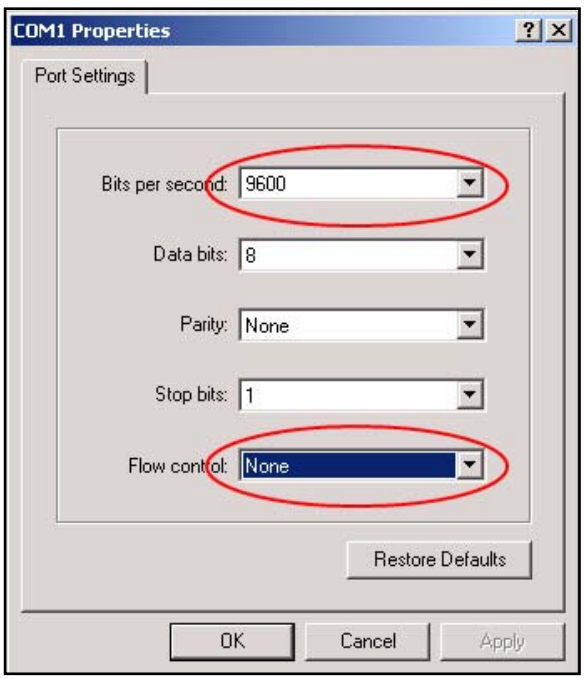


Fig 1-5 Opening HyperTerminal (4)

Step 3 Entering switch CLI interface:

Power on the switch. The following appears in the HyperTerminal windows, that is the CLI configuration mode for ES4626.

ES4626 Management Switch

Copyright (c) 2001-2004 by Accton Technology Corporation.
All rights reserved.

Reset chassis ... done.
Testing RAM...
134,217,728 RAM OK.

Initializing...
Attaching to file system ... done.

Loading nos.img ... done.
Starting at 0x10000...

Current time is WED APR 20 09: 37: 52 2005

ES4626 Series Switch Operating System, Software Version ES4626 1.1.0.0,
Copyright (C) 2001-2006 by Accton Technology Corporation
http: //www.edge-core. com.

ES4626 Switch
26 Ethernet/IEEE 802.3 interface(s)

Press ENTER to start session

The user can now enter commands to manage the switch. For a detailed description for the commands, please refer to the following chapters.

1.1.2 In-band Management

In-band management refers to the management by login to the switch using Telnet. In-band management enables management of the switch for some devices attached to

the switch. In the case when in-band management fails due to switch configuration changes, out-of-band management can be used for configuring and managing the switch.

1.1.2.1 Management via Telnet

To manage the switch with Telnet, the following conditions should be met:

1) Switch has an IP address configured
2) The host IP address (Telnet client) and the switch's VLAN interface IP address is in the same network segment.
3) If not 2), Telnet client can connect to an IP address of the switch via other devices, such as a router.

ES4626/ES4650 is a Layer 3 switch that can be configured with several IP addresses. The following example assumes the shipment status of the switch where only VLAN1 exists in the system.

The following describes the steps for a Telnet client to connect to the switch's VLAN1 interface by Telnet.

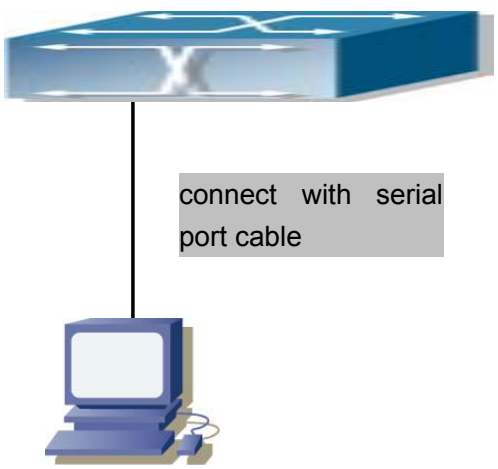


Fig 1-6 Manage the switch by Telnet

Step 1: Configure the IP addresses for the switch

First is the configuration of host IP address. This should be within the same network segment as the switch VLAN1 interface IP address. Suppose the switch VLAN interface IP address 10.1.128.251/24. Then, a possible host IP address is 10.1.128.252/24. Run "ping 10.1.128.251" from the host and verify the result, check for reasons if ping failed.

The IP address configuration commands for VLAN1 interface are listed below. Before in-band management, the switch must be configured with an IP address by out-of-band

management (i.e. Console mode), The configuration commands are as follows (All switch configuration prompts are assumed to be “switch” hereafter if not otherwise specified):

Switch>
Switch>en
Switch#config
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-If-Vlan1)#no shutdown

Step 2: Run Telnet Client program.

Run Telnet client program included in Windows with the specified Telnet target.

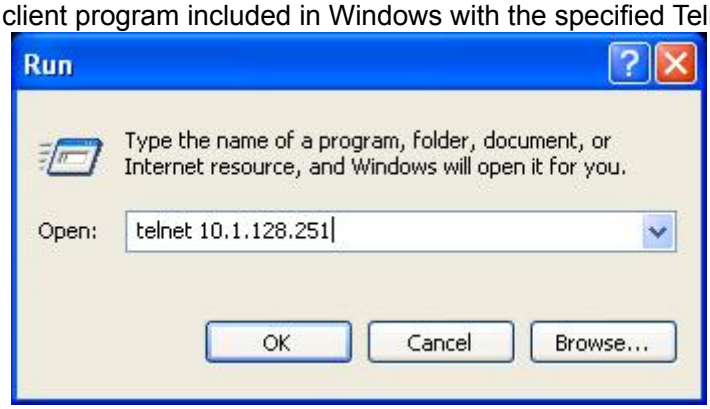


Fig 1-7 Run telnet client program included in Windows

Step 3: Login to the switch

Login to the Telnet configuration interface. Valid login name and password are required, otherwise the switch will reject Telnet access. This is a method to protect the switch from unauthorized access. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command:

telnet-user <user> password {0|7} <password>.

Assume an authorized user in the switch has a username of “test”, and password of “test”, the configuration procedure should like the following:

Switch>en
Switch#config
Switch(Config)#telnet-user test password 0 test

Enter valid login name and password in the Telnet configuration interface, Telnet user

will be able to enter the switch's CLI configuration interface. The commands used in the Telnet CLI interface after login is the same as in that in the Console interface.

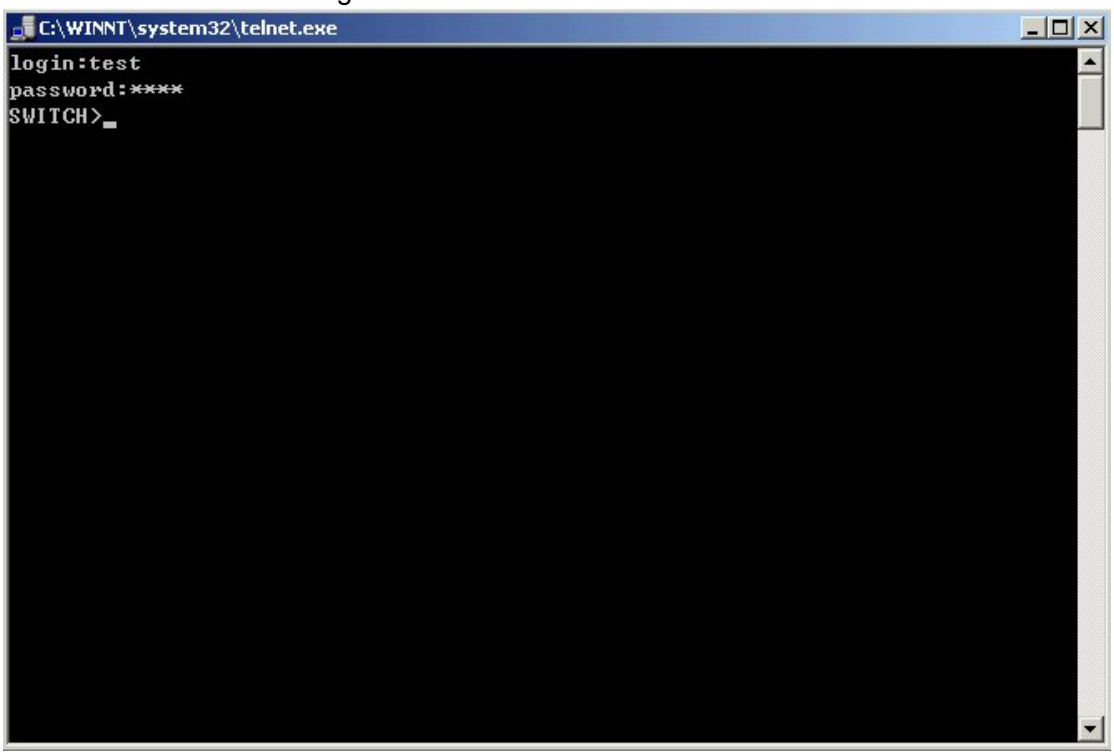


Fig 1-8 Telnet Configuration Interface

1.1.2.2 Management via HTTP

To manage the switch via HTTP, the following conditions should be met:

1) Switch has an IP address configured
2) The host IP address (HTTP client) and the switch's VLAN interface IP address are in the same network segment;
3) If 2) is not met, HTTP client should connect to an IP address of the switch via other devices, such as a router.

Similar to management via Telnet, as soon as the host succeeds to ping an IP address of the switch and to type the right login password, it can access the switch via HTTP. The configuration sequence is as below:

Step 1: Configure the IP addresses for the switch and start the HTTP function on the switch.

For configuring the IP address on the switch through out-of-band management, see the relevant chapter.

To enable the WEB configuration, users should type the CLI command **ip http server** in the global mode as below:

Switch>en

Switch#config

Switch(Config)#ip http server

Step 2: Run HTTP protocol on the host.

Open the Web browser on the host and type the IP address of the switch. Or run directly the HTTP protocol on the Windows. For example, the IP address of the switch is “10.1.128.251”.

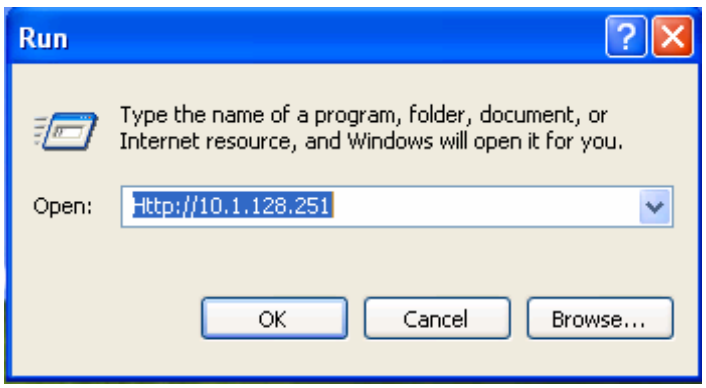


Fig 1-9 Run HTTP Protocol

Step 3: Logon to the switch

To logon to the HTTP configuration interface, valid login user name and password are required; otherwise the switch will reject HTTP access. This is a method to protect the switch from the unauthorized access. Consequently, in order to configure the switch via HTTP, username and password for authorized HTTP users must be configured with the following command in the global mode:

username *<username>* password *<show_flag>* *<password>*. Suppose an authorized user in the switch has a username as “test”, and password as “test”. The configuration procedure is as below:

Switch>en

Switch#config

Switch(Config)# username test password 0 test

The Web login interface is as below:

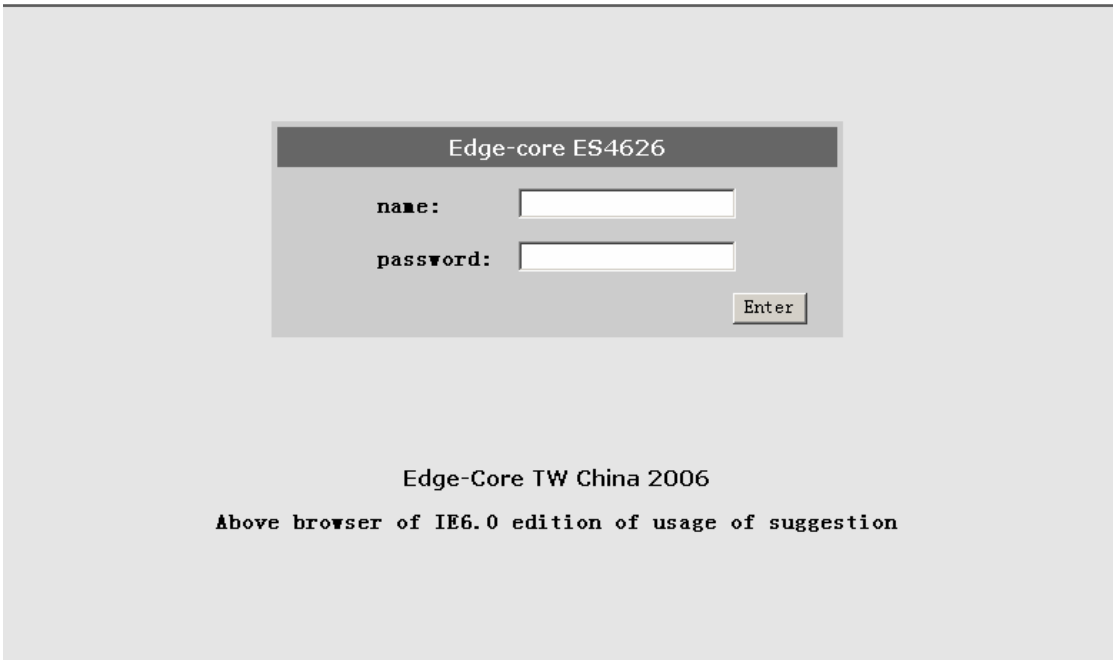


Fig 1-10 Web Login Interface

Input the right username and password, and then the main Web configuration interface is shown as below.

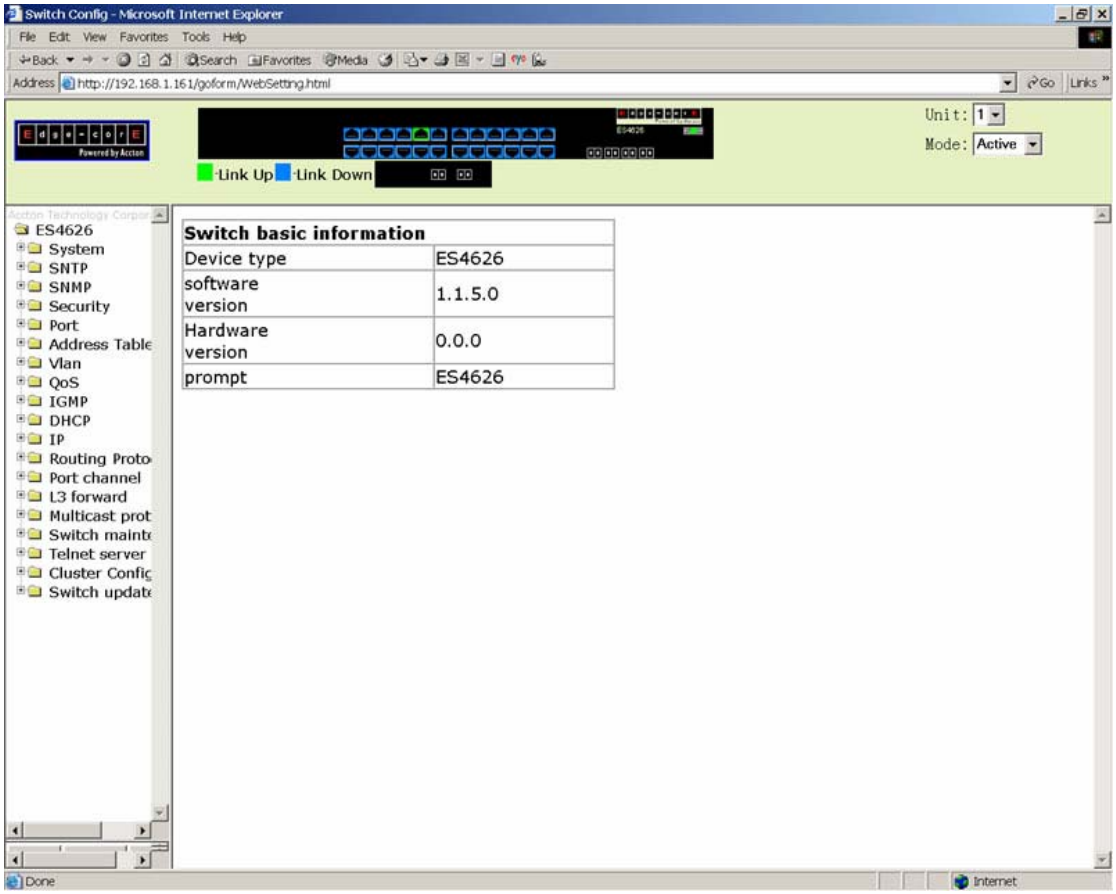


Fig 1-11 Main Web Configuration Interface

1.2 Management Interface

1.2.1 CLI Interface

CLI interface is familiar to most users. As aforementioned, out-of-band management and Telnet login are all performed through CLI interface to manage the switch.

CLI Interface is supported by Shell program, which consists of a set of configuration commands. Those commands are categorized according to their functions in switch configuration and management. Each category represents a different configuration mode. The Shell for the switch is described below:

- Configuration Modes
- Configuration Syntax
- Shortcut keys
- Help function

- Input verification
- Fuzzy match support

1.2.1.1 Configuration Modes

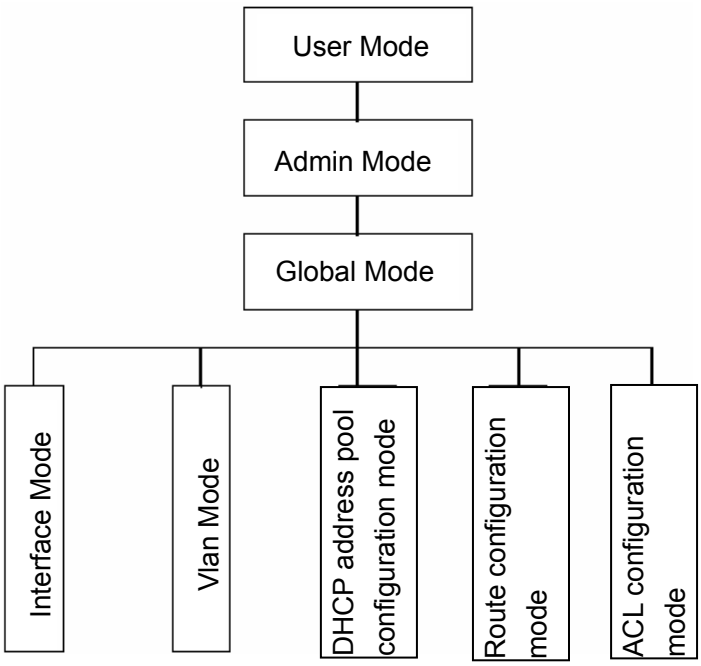


Fig 1-12 Shell Configuration Modes

1.2.1.1.1 User Mode

On entering the CLI interface, entering user entry system first. If as common user, it is defaulted to User Mode. The prompt shown is “Switch>”, the symbol “>” is the prompt for User Mode. When **disable** command is run under Admin Mode, it will also return to the User Mode.

Under User Mode, no configuration to the switch is allowed, only clock time and version information of the switch can be queries.

1.2.1.1.2 Admin Mode

To enter Under Admin Mode see the following: In user entry system, if as Admin user, it is defaulted to Admin Mode. Admin Mode prompt “Switch#” can be entered under the User Mode by running the *enable* command and entering corresponding access levels admin user password, if a password has set. Or, when *exit* command is run under Global

Mode, it will also return to the Admin Mode. ES4626/ES4650 also provides a shortcut key sequence "Ctrl+z", this allows an easy way to exit to Admin Mode from any configuration mode (except User Mode).

Under Admin Mode, when disable command is run, it will return to User Mode. When exit command is run, it will exit the entry and enter user entry system direct. Next users can reenter the system on entering corresponding user name and password.

Under Admin Mode, the user can query the switch configuration information, connection status and traffic statistics of all ports; and the user can further enter the Global Mode from Admin Mode to modify all configurations of the switch. For this reason, a password must be set for entering Admin mode to prevent unauthorized access and malicious modification to the switch.

1.2.1.1.3 Global Mode

Type the *config* command under Admin Mode will enter the Global Mode prompt "Switch(Config)#". Use the *exit* command under other configuration modes such as Interface Mode, VLAN mode will return to Global Mode.

The user can perform global configuration settings under Global Mode, such as MAC Table, Port Mirroring, VLAN creation, IGMP Snooping start, GVRP and STP, etc. And the user can go further to Interface Mode for configuration of all the interfaces.

1.2.1.1.3.1 Interface Mode

Use the *interface* command under Global Mode can enter the interface mode specified. ES4626/ES4650 provides three interface type: VLAN interface, Ethernet port and port-channel, and accordingly the three interface configuration modes.

Interface Type	Entry	Prompt	Operates	Exit
VLAN Interface	Type ***interface vlan <Vlan-id>*** command under Global Mode.	**Switch(Config-If-Vlanx)#**	Configure switch IPs, etc	Use the *exit* command to return to Global Mode.
Ethernet Port	Type ***interface ethernet <interface-list>*** command under Global Mode.	**Switch(Config-ethernetxx)#**	Configure supported duplex mode, speed, etc. of Ethernet Port.	Use the *exit* command to return to Global Mode.
port-channel	Type ***interface***	**Switch(Config-if-**	Configure	Use the *exit*

	port-channel <port-channel-number> command under Global Mode.	**port-channelx)#**	port-channel related settings such as duplex mode, speed, etc.	command to return to Global Mode.

1.2.1.1.3.2 VLAN Mode

Using the *vlan <vlan-id>* command under Global Mode can enter the corresponding VLAN Mode. Under VLAN Mode the user can configure all member ports of the corresponding VLAN. Run the *exit* command to exit the VLAN Mode to Global Mode.

1.2.1.1.3.3 DHCP Address Pool Mode

Type the ***ip dhcp pool <name>*** command under Global Mode will enter the DHCP Address Pool Mode prompt "**Switch(Config-<name>-dhcp)#**". DHCP address pool properties can be configured under DHCP Address Pool Mode. Run the *exit* command to exit the DHCP Address Pool Mode to Global Mode.

1.2.1.1.3.4 Route Mode

Routing Protocol	Entry	Prompt	Operates	Exit
RIP Routing Protocol	Type ***router rip*** command under Global Mode.	**Switch(Config-Router-Rip)#**	Configure RIP protocol parameters.	Use the "*exit*" command to return to Global Mode.
OSPF Routing Protocol	Type ***router ospf*** command under Global Mode.	**Switch(Config-Router-Ospf)#**	Configure OSPF protocol parameters.	Use the "*exit*" command to return to Global Mode.

1.2.1.1.3.5 ACL Mode

ACL type	Entry	Prompt	Operates	Exit
Standard IP ACL Mode	Type **access-list ip** command under Global Mode.	**Switch(Config-Std-Nacl-a)#**	Configure parameters for Standard IP ACL Mode	Use the "*exit*" command to return to Global Mode.
Extended IP ACL Mode	Type **access-list ip** command under Global Mode.	**Switch(Config-Ext-Nacl-b)#**	Configure parameters for Extended IP ACL Mode	Use the "*exit*" command to return to Global Mode.

1.2.1.2 Configuration Syntax

ES4626/ES4650 provides various configuration commands. Although all the commands are different, they all abide by the syntax for ES4626/ES4650 configuration commands. The general command format of ES4626/ES4650 is shown below:

cmdtxt <*variable*> { enum1 | … | enumN } [option]

Conventions: **cmdtxt** in bold font indicates a command keyword; **<*variable*>** indicates a variable parameter; **{enum1 | … | enumN }** indicates a mandatory parameter that should be selected from the parameter set **enum1~enumN**; and the square bracket ([ ]) in **[option]** indicate a optional parameter. There may be combinations of "< >", "{ }" and "[ ]" in the command line, such as **[<*variable*>]**,**{enum1 <*variable*>| enum2}**, **[option1 [option2]], etc.**

Here are examples for some actual configuration commands:

- **show calendar**, no parameters required. This is a command with only a keyword and no parameter, just type in the command to run.
- **vlan <*vlan-id*>**, parameter values are required after the keyword.
- **duplex {auto|full|half}**，user can enter *duplex half*, *duplex full* or *duplex auto* for this command.
- **snmp-server community <*string*>{ro|rw}**, the followings are possible:
  snmp-server community <*string*> ro
  snmp-server community <*string*> rw

1.2.1.3 Shortcut Key Support

ES4626/ES4650 provides several shortcut keys to facilitate user configuration, such as up, down, left, right and Blank Space. If the terminal does not recognize Up and Down keys, ctrl+p and ctrl+n can be used instead.

<table>
<tr><td>Key(s)</td><td colspan="2">Function</td></tr>
<tr><td>BackSpace</td><td colspan="2">Delete a character before the cursor, and the cursor moves back.</td></tr>
<tr><td>Up “↑”</td><td colspan="2">Show previous command entered. Up to ten recently entered commands can be shown.</td></tr>
<tr><td>Down “↓”</td><td colspan="2">Show next command entered. When use the Up key to get previously entered commands, you can use the Down key to return to the next command</td></tr>
<tr><td>Left “←”</td><td>The cursor move one character to the left.</td><td rowspan="2">You can use the Left and Right key to modify an entered command.</td></tr>
<tr><td>Right “→”</td><td>The cursor moves one character to the right.</td></tr>
<tr><td>Ctr+p</td><td colspan="2">The same as Up key “↑”.</td></tr>
<tr><td>Ctr+n</td><td colspan="2">The same as Down key “↓”.</td></tr>
<tr><td>Ctr+b</td><td colspan="2">The same as Left key “←”.</td></tr>
<tr><td>Ctr+f</td><td colspan="2">The same as Right key “→”.</td></tr>
<tr><td>Ctr+z</td><td colspan="2">Return to the Admin Mode directly from the other configuration modes (except User Mode).</td></tr>
<tr><td>Ctr+c</td><td colspan="2">Break the ongoing command process, such as ping or other command execution.</td></tr>
<tr><td>Tab</td><td colspan="2">When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.</td></tr>
</table>

1.2.1.4 Help function

There are two ways in ES4626/ES4650 for the user to access help information: the “help” command and the “?”.

Access to Help	Usage and function
Help	Under any command line prompt, type in “help” and press Enter will get a brief description of the associated help system.

“?”	1.Under any command line prompt, enter “?” to get a command list of the current mode and related brief description. 2.Enter a “?” after the command keyword with a embedded space. If the position should be a parameter, a description of that parameter type, scope, etc, will be returned; if the position should be a keyword, then a set of keywords with brief description will be returned; if the output is “<cr>”, then the command is complete, press Enter to run the command. 3.A “?” immediately following a string. This will display all the commands that begin with that string.

1.2.1.5Input verification

1.2.1.5.1 Returned Information: success

All commands entered through keyboards undergo syntax check by the Shell. Nothing will be returned if the user entered a correct command under corresponding modes and the execution is successful.

1.2.1.5.2 Returned Information: error

Output error message	Explanation
Unrecognized command or illegal parameter!	The entered command does not exist, or there is error in parameter scope, type or format.
Ambiguous command	At least two interpretations is possible basing on the current input.
Invalid command or parameter	The command is recognized, but no valid parameter record is found.
This command is not exist in current mode	The command is recognized, but this command can not be used under current mode.
Please configure precursor command "*" at first !	The command is recognized, but the prerequisite command has not been configured.
syntax error : missing "" before the end of command line!	Quotation marks are not used in pairs.

1.2.1.6 Fuzzy match support

ES4626/ES4650 Shell support fuzzy match in searching command and keyword. Shell will recognize commands or keywords correctly if the entered string causes no conflict.

For example:

1. For Admin configuration command “show interfaces status ethernet 1/1”, typing “sh in status e 1/1” will work
2. However, for Admin configuration command “show running-config”, the system will report a “> Ambiguous command!” error if only “show r” is entered, as Shell is unable to tell whether it is “show rom” or “show running-config”. Therefore, Shell will only recognize the command if “sh ru” is entered.

1.2.2WEB Interface

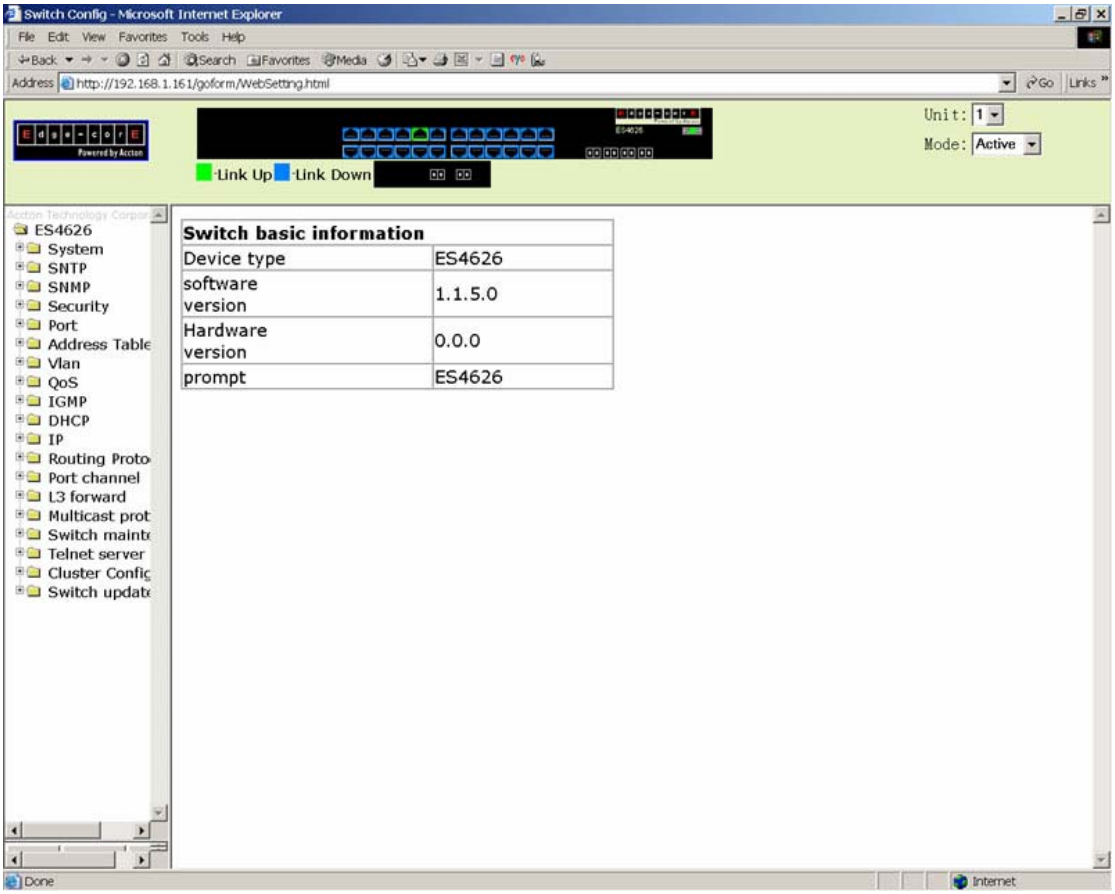
ES4626/ES4650 has HTTP Web management function. Users can configure and examine the switch through a Web browser.

By conducting the following configurations, users can realize the Web management.

1. Configure valid IP address, network mask and default gateway for the switch. See 5.3
2. Configure management user name and password.
3. Establish a connection to the switch through Web browser. Input username and password. Then users can manage the switch through Web browser.

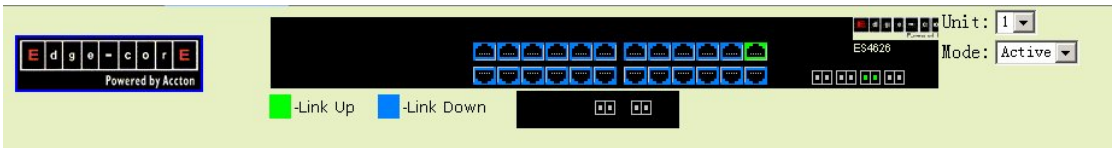
1.2.2.1Main page

After passing the authentication by inputting username and password, users can see the management page as below. On the management page, the main menu is on the left and the system information and parameters are shown on the right. Click the links on the main menu, users can see the corresponding configuration statistics.



1.2.2.2 Interface Panel

On the top of the management page, the switch interface shows the current status of the ports. Click the ports which are in the state of “Link Up”, the port statistics are shown on the right.



Chapter 2 Basic Switch Configuration

2.1 Basic Switch Configuration Commands

The basic configuration for the switch including all the commands for entering and exiting the Admin Mode and Interface Mode, setting and displaying switch clock and displaying system version information.

2.1.1calendar set

Command: calendar set *<HH> <MM> <SS> {<DD> <MON> <YYYY> | <MON> <DD> <YYYY>}*

Function: Set system date and time.

Parameter: *<HH> <MM> <SS>* is the current time, and the valid scope for ***HH*** is 0 to 23, ***MM*** and ***SS*** 0 to 59; ***<DD> <MON> <YYYY>*** or ***<MON> <DD> <YYYY>*** is the current date, month and year or the current year, month and date, and the valid scope for ***YYYY*** is 1970~2100, ***MON*** meaning month, and ***DD*** between 1 to 31.

Command mode: Admin Mode

Default: upon first time start-up, it is defaulted to 2001.1.1 0: 0: 0.

Usage guide: The switch can not continue timing with power off, hence the current date and time must be first set at environments where exact time is required.

Example: To set the switch current date and time to 2002.8.1 23: 0: 0:

Switch# calendar set 23 0 0 august 1 2002Related command: show calendar

2.1.2 config

Command: config [terminal]

Function: Enter Global Mode from Admin Mode.

Parameter: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

2.1.3 enable

Command: enable

Function: Enter Admin Mode from User Mode.

Parameter: 0 and 15 are user access levels. 0 is normal user level. In this level, users can enter Admin Mode and conduct major commands such as show, ping and traceroute etc. But users can't enter Global Mode. 15 is privileged user level. In this level, users can conduct all the command of this level. ***<password>*** is password for logging on to the privileged user mode.

Command mode: User Mode

Default: If users don't specify the level, the default level is 15.

Usage Guide: To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. Set the Admin user password under Global Mode with "**enable password**" command.

Example:

Switch>enable

password: ***** (admin)

Switch#

Related command: enable password

2.1.4 disable

Command: disable

Function: Enter User Mode from Admin Mode.

Command mode: Admin Mode

Example:

Switch#disable

Switch>

Related command: enable

2.1.5 enable password

Command: enable password**[level {0 | 15}]**

Function: Modify the password to enter Admin Mode from the User Mode, press Enter after type in this command displays ***<Current password>*** and ***<New password>*** parameter for the users to configure.

Parameter: 0 is normal user access level, users can enter Admin Mode and conduct major commands such as show, ping and trace route etc. But users can't enter Global Mode. 15 is privileged user level. In this level, users can conduct all the command of this level. ***<Current password>*** is the original password, up to 16 characters are allowed; ***<New password>*** is the new password, up to 16 characters are allowed; ***<Confirm new password>*** is to confirm the new password and should be the same as ***<New password>***, otherwise, the password will need to be set again.

Command mode: Global Mode

Default: If users don't specify the level, the default level is 15,upon first time start-up, the Admin user password is empty. If this is the first configuration, simply press Enter on prompting for current password.

Usage Guide: Configure Admin user password to prevent unauthorized access from non-admin user. It is recommended to set the Admin user password at the initial switch configuration. Also, it is recommended to exit Admin Mode with "**exit**" command when the administrator needs to leave the terminal for a long time.

Example: Set the Admin user password to "admin".

Switch(Config)#enable password

Current password: (First time configuration, no password set, just press Enter)

New password: ***** (Type in admin to set the new password to "admin")

Confirm New password: ***** (Type admin again to confirm the new password)

Switch(Config)#

Related command: enable

2.1.6 exec timeout

Command: exec timeout <*minutes* >

Function: Set timeout value for exiting Admin Mode

Parameter: < *minute* > is the time in minutes, the valid range is 0 to 300.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: To ensure security for the switch and prevent malicious operation of unauthorized user, timeout count will start after the last configuration by the Admin user. And the system will automatically exit the Admin Mode upon preset timeout threshold. If the user needs to enter Admin Mode, Admin user password needs to be entered again. A

0 exec timeout value indicate the system will never exit Admin Mode automatically.

Example: Set timeout value for the switch to exit Admin Mode to 6 minutes.

Switch(Config)#exec timeout 6

2.1.7 exit

Command: exit

Function: Exit the current mode to the previous mode. Under Global Mode, this command will return the user to Admin Mode, and in Admin Mode to User Mode, etc.

Command mode: All configuration modes.

Example:

Switch#exit

Switch>

2.1.8 help

Command: help

Function: Output brief description of the command interpreter help system.

Command mode: All configuration modes.

Usage Guide: An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in ? any time to get online help.

Example:

Switch>help

enable	-- Enable Privileged mode
exit	-- Exit telnet session
help	-- help
show	-- Show running system information

2.1.9 ip host

Command: ip host <hostname> <ip_addr>

no ip host <*hostname*>

Function: Set the mapping relationship between the host and IP address; the “no ip host”

parameter of this command will delete the mapping.

Parameter: <*hostname*> is the host name, up to 15 characters are allowed; **<*ip_addr*>** is the corresponding IP address for the host name, takes a dot decimal format.

Command mode: Global Mode

Usage Guide: Set the association between host and IP address, which can be used in commands like **"ping <host>**".

Example: Set IP address of a host with the hostname of "beijing" to 200.121.1.1.

Switch(Config)#ip host beijing 200.121.1.1

Related commands: telnet、ping、traceroute

2.1.10 hostname

Command: hostname <*hostname*>

Function: Set the prompt in the switch command line interface.

Parameter **<*hostname*>** is the string for the prompt, up to 30 characters are allowed.

Command mode: Global Mode

Default: The default prompt is ES4626/ES4650.

Usage Guide: With this command, the user can set the command line prompt of the switch according to their own requirements.

Example: Set the prompt to "Test".

Switch(Config)#hostname Test

Test(Config)#

2.1.11 username password

Command: username <*user_name*> password <*show_flag*> <*pass_word*>

no uername <*user_name*>

Function: Configure username and password for logging on the switch; the "**no username <*user_name*>**" command deletes the user.

Parameter: <*user_name*> is the username. It can't exceed 16 characters; **<*show_flag*>** can be either 0 or 7. 0 is used to display unencrypted username and password, whereas 7 is used to display encrypted username and password; **<*pass_word*>** is password. It can't exceed 16 characters;

Command mode: Global Mode

Default: The username and password are null by default.

Usage Guide: This command can be used to set the username for logging on the switch and set the password as null.

Example: Set username as “admin” and set password as “admin”

Switch(Config)#username admin password 0 admin

Switch(Config)#

Related Command: username nopassword、username access-level、show users

2.1.12 username nopassword

Command: username <*user_name*> nopassword

Function: Set the username for logging on the switch and set the password as null.

Parameter: <*user_name*> is the username. It can’t exceed 16 characters.

Command mode: Global Mode

Usage Guide: This command is used to set the username for logging on the switch and set the password as null.

Example: Set username as “admin” and set password as null.

Switch(Config)#username admin nopassword

Switch(Config)#

Related Command: username password、username access-level、show users

2.1.13 username access-level

Command: username <*user_name*> access-level <*level*>

Function: Configure the access level for users who log on the switch.

Parameter: <*user_name*> is the username. It can’t exceed 16 characters; **<*level*>** can be either 0 or 15. 0 is normal user level and 15 is privileged user level.

Command mode: Global Mode

Example: Create user “admin” and set the level of this user as privileged user level.

Switch(Config)#username admin access-level 15

Switch(Config)#

Related Command: username password、username nopassword、show users

2.1.14 reload

Command: reload

Function: Warm reset the switch.

Command mode: Admin Mode

Usage Guide: The user can use this command to restart the switch without power off .

2.1.15 set default

Command: set default

Function: Reset the switch to factory settings.

Command mode: Admin Mode

Usage Guide: Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.

Note: After the command, "**write**" command must be executed to save the operation. The switch will reset to factory settings after restart.

Example:

Switch#set default

Are you sure? [Y/N] = y

Switch#write

Switch#reload

2.1.16 setup

Command: setup

Function: Enter the Setup Mode of the switch.

Command mode: Admin Mode

Usage Guide: ES4626/ES4650 provides a Setup Mode, in which the user can configure IP addresses, etc.

2.1.17 language

Command: language {chinese|english}

Function: Set the language for displaying the help information.

Parameter: chinese for Chinese display; **english** for English display.

Command mode: Admin Mode

Default: The default setting is English display.

Usage Guide: ES4626/ES4650 provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information display will revert to English.

2.1.18 write

Command: write

Function: Save the currently configured parameters to the Flash memory.

Command mode: Admin Mode

Usage Guide: After a set of configuration with desired functions, the setting should be saved to the Flash memory, so that the system can revert to the saved configuration automatically in the case of accidentally powered down or power failure. This is the equivalent to the **copy running-config startup-config** command.

Related commands: copy running-config startup-config

2.2 Maintenance and Debug Commands

When the users configures the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in network failure, the users will also need to diagnostic the problem. ES4626/ES4650 provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

2.2.1 ping

Command: ping [<*ip-addr*>]

Function: The switch send ICMP packet to remote devices to verify the connectivity between the switch and remote devices.

Parameter: <*ip-addr*> is the target host IP address for ping, in dot decimal format.

Default: Send 5 ICMP packets of 56 bytes each, timeout in 2 seconds.

Command mode: Admin Mode

Usage Guide: When the user types in the **ping** command and press Enter, the system will provide an interactive mode for configuration, and the user can choose all the parameters for **ping**.

Example:

Example 1: Default parameter for **ping.**

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

As shown in the above example, the switch pings a device with an IP address of 10.1.128.160, three ICMP request packets sent without receiving corresponding reply

packets (i.e. ping failed), the last two packets are replied successfully, the successful rate is 40%. The switch represent ping failure with a ".", for unreachable target; and ping success with "!" , for reachable target.

Switch#ping
protocol [IP]:
Target IP address: 10.1.128.160
Repeat count [5]: 100
Datagram size in byte [56]: 1000
Timeout in milli-seconds [2000]: 500
Extended commands [n]: n

Displayed information	Explanation
protocol [IP]:	Select the **ping** for IP protocol
Target IP address:	Target IP address
Repeat count [5]	Packet number, the default is 5
Datagram size in byte [56]	ICMP packet size the default is 56 bytes
Timeout in milli-seconds [2000]:	Timeout (in milliseconds,) the default is 2 seconds.
Extended commands [n]:	Whether to change the other options or not

2.2.2 Telnet

2.2.2.1 Introduction to Telnet

Telnet is a simple remote terminal protocol for remote login. Using Telnet, the user can login to a remote host with its IP address of hostname from his own workstation. Telnet can send the user's keystrokes to the remote host and send the remote host output to the user's screen through TCP connection. This is a transparent service, as to the user, the keyboard and monitor seems to be connected to the remote host directly.

Telnet employs the Client-Server mode, the local system is the Telnet client and the remote host is the Telnet server. ES4626/ES4650 can be either the Telnet Server or the Telnet client.

When ES4626/ES4650 is used as the Telnet server, the user can use the Telnet client program included in Windows or the other operation systems to login to ES4626/ES4650, as described earlier in the In-band management section. As a Telnet server, ES4626/ES4650 allows up to 5 telnet client TCP connections.

And as Telnet client, use **telnet** command under Admin Mode allow the user to login to the other remote hosts. ES4626/ES4650 can only establish TCP connection to one

remote host. If a connection to another remote host is desired, the current TCP connection must be dropped.

2.2.2.2 Telnet Task Sequence

1. Configuring Telnet Server
2. Telnet to a remote host from the switch.

1. Configuring Telnet Server

Command	Explanation
Global Mode	
ip telnet server **no ip telnet server**	Enable the Telnet server function in the switch: the "no **telnet-server enable"** command disables the Telnet function.
telnet-server securityip <*ip-addr*> **no telnet-server securityip <*ip-addr*>**	Configure the secure IP address to login to the switch through Telnet: the "**no telnet-server securityip <*ip-addr*>" command deletes the authorized Telnet secure address.**
Admin Mode	
monitor **no monitor**	Display debug information for Telnet client login to the switch; the "**no monitor" command disables the** debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
telnet [<*ip-addr*>] [<*port*>]	Login to a remote host with the Telnet client included in the switch.

2.2.2.3 Telnet Commands

2.2.2.3.1 monitor

Command: monitor

no monitor

Function: Enable debug information for Telnet client login to the switch, the Console end debug display will be disabled at the same time; the “no monitor” command disables the debug information and re-enables the Console end debug display. .

Command mode: Admin Mode

Usage Guide: When Telnet client accessing the switch enables Debug information, the information is not shown in the Telnet interface, instead, it is displayed in the terminal connecting to the Console port. This command specifies the debug information to be displayed in the Telnet terminal screen instead of the Console or the other Telnet terminal screens.

Example: Enable displaying the debug information in Telnet client.

Switch#monitor

2.2.2.3.2 telnet

Command: telnet [<*ip-addr*>] [<*port*>]

Function: Login to a remote host with an IP address of ***<ip-addr>*** through Telnet.

Parameter: *<ip-addr>* is the remote host IP address in dot decimal format. ***<port>*** is the port number, valid value is 0 – 65535.

Command mode: Admin Mode

Usage Guide: This command is used when the switch is used as a client, the user logs in to remote hosts for configuration with this command. ES4626/ES4650 can only establish TCP connection to one remote host as the Telnet client. If a connection to another remote host is desired, the current TCP connection must be dropped. To disconnect with a remote host, the shortcut key combination “CTRL+|” can be used.

Input **Telnet** keyword without any parameter enters the Telnet configuration mode.

Example: Telnet to a remote router with the IP address 20.1.1.1 from the switch.

Switch#telnet 20.1.1.1 23

Connecting Host 20.1.1.123 Port 23...

Service port is 23

Connected to 20.1.1.123login: 123

password: ***

route>

2.2.2.3.3 ip telnet server

Command: ip telnet server

no ip telnet server

Function: Enable the Telnet server function in the switch: the "**no telnet-server enable"** command disables the Telnet function in the switch.

Default: Telnet server function is enabled by default.

Command mode: Global Mode

Usage Guide: This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch.

Example: Disable the Telnet server function in the switch.

Switch(Config)#no telnet-server enable

2.2.2.3.4 telnet-server securityip

Command: telnet-server securityip <*ip-addr*>

no telnet-server securityip <*ip-addr*>

Function: Configure the secure IP address of Telnet client allowed to login to the switch; the "**no telnet-server securityip <*ip-addr*>" command deletes the authorized Telnet secure address.**

Parameter: <*ip-addr*> is the secure IP address allowed to access the switch, in dot decimal format.

Default: no secure IP address is set by default.

Command mode: Global Mode

Usage Guide: When no secure IP is configured, the IP addresses of Telnet clients connecting to the switch will not be limited; if a secure IP address is configured, only hosts with the secure IP address is allowed to connect to the switch through Telnet for configuration. The switch allows multiple secure IP addresses.

Example: Set 192.168.1.21 as a secure IP address.

Switch(Config)#telnet-server securityip 192.168.1.21

2.2.3SSH

2.2.3.1Introduction to SSH

SSH (Secure Shell) is a protocol which ensures a secure remote access connection to network devices. It is based on the reliable TCP/IP protocol. By conducting the mechanism such as key distribution, authentication and encryption between SSH server and SSH client, a secure connection is established. The information transferred on this

connection is protected from being intercepted and decrypted. The switch meets the requirements of SSH2.0. It supports SSH2.0 client software such as SSH Secure Client and putty. Users can run the above software to manage the switch remotely.

The switch presently supports RSA authentication, 3DES cryptography protocol and SSH user password authentication etc.

2.2.3.2SSH Server Configuration Sequence

1. SSH Server Configuration

Command	Explanation
Global Mode	
ssh-server enable **no ssh-server enable**	Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
ssh-user <*user-name*> password {0|7} <*password*> **no ssh-user <*user-name*>**	Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.
ssh-server timeout <*timeout*> **no ssh-server timeout**	Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.
ssh-server authentication-retires < *authentication-retires*> **no ssh-server authentication-retries**	Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.
ssh-server host-key create rsa modulus <*moduls*>	Generate the new RSA host key on the SSH server.
Admin Mode	
monitor **no monitor**	Display SSH debug information on the SSH client side; the "**no monitor**" command stops displaying SSH debug information on the SSH client side.

2.2.3.3 SSH Configuration Commands

2.2.3.3.1 ssh-server enable

Command: ssh-server enable

no ssh-server enable

Function: Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.

Command mode: Global Mode

Default: SSH function is disabled by default.

Usage Guide: In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch.

Example: Enable SSH function on the switch.

Switch(Config)#ssh-server enable

2.2.3.3.2 ssh-user

Command: ssh-user *<username>* password {0|7} *<password>*

no ssh-user *<username>*

Function: Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.

Parameter: *<username>* is SSH client username. It can't exceed 16 characters; ***<password>*** is SSH client password. It can't exceed 8 characters; **0|7** stand for unencrypted password and encrypted password.

Command mode: Global Mode

Default: There are no SSH username and password by default.

Usage Guide: This command is used to configure the authorized SSH client. Any unauthorized SSH clients can't log on and configure the switch. When the switch is a SSH server, it can have maximum three users and it allows maximum three users to connect to it at the same time.

Example: Set a SSH client which has "switch" as username and "switch" as password.

Switch(Config)#ssh-user switch password 0 switch

2.2.3.3.3 ssh-server timeout

Command: ssh-server timeout *<timeout>*

no ssh-server timeout

Function: Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.

Parameter: <*timeout*> is timeout value; valid range is 10 to 600 seconds.

Command mode: Global Mode

Default: SSH authentication timeout is 180 seconds by default.

Example: Set SSH authentication timeout to 240 seconds.

Switch(Config)#ssh-server timeout 240

2.2.3.3.4 ssh-server authentication-retries

Command: ssh-server authentication-retries < authentication-retries >

no ssh-server authentication-retries

Function: Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.

Parameter: < authentication-retries > is the number of times for retrying authentication; valid range is 1 to 10.

Command mode: Global Mode

Default: The number of times for retrying SSH authentication is 3 by default.

Example: Set the number of times for retrying SSH authentication to 5.

Switch(Config)#ssh-server authentication-retries 5

2.2.3.3.5 ssh-server host-key create rsa

Command: ssh-server host-key create rsa [modulus < modulus >]

Function: Generate new RSA host key

Parameter: modulus is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.

Command mode: global Mode

Default: The system uses the key generated when the ssh-server is started at the first time.

Usage Guide: This command is used to generate the new host key. When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and "write" command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.

Example: Generate new host key.

Switch(Config)#ssh-server host-key create rsa

2.2.3.3.6 monitor

Command: monitor

no monitor

Function: Display SSH debug information on the SSH client side and stop displaying SSH debug information on the Console; the "**no monitor**" command stops displaying SSH debug information on the SSH client side and enables to display SSH debug information on the Console.

Command mode: Admin Mode

Usage Guide: When SSH client accesses the switch and users enable to display SSH Debug information, this information is displayed on the Console terminal instead of SSH interface. This command enables debug information to be displayed on the SSH interface instead of on the Console terminal.

Example: Enable to display SSH debug information on the SSH client interface.

Switch#monitor

Related command: ssh-user

2.2.3.4Typical SSH Server Configuration

Example 1:

Requirement: Enable SSH server on the switch, and run SSH2.0 client software such as Secure shell client and putty on the terminal. Log on the switch by using the username and password from the client.

Configure the IP address, add SSH user and enable SSH service on the switch. SSH2.0 client can log on the switch by using the username and password to configure the switch.

Switch(Config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 100.100.100.200 255.255.255.0
Switch(Config-Vlan-1)#exit
Switch(Config)#ssh-user test password 0 test
Switch(Config)#ssh-server enable

2.2.3.5SSH Monitor and Debug Commands

2.2.3.5.1 show ssh-user

Command: show ssh-user

Function: Display the configured SSH usernames.

Parameter: Admin Mode

Example:

Switch#show ssh-user

test

Related command: ssh-user

2.2.3.5.2 show ssh-server

Command: show ssh-server

Function: Display SSH state and users which log on currently.

Command mode: Admin Mode

Example:

Switch#show ssh-server

ssh-server is enabled

connection version state user name

1 2.0 session started test

Related command: ssh-server enable, no ssh-server enable

2.2.3.5.3 debug ssh-server

Command: debug ssh-server

no debug ssh-server

Function: Display SSH server debugging information; the "**no debug ssh-server**" command stops displaying SSH server debugging information.

Default: This function is disabled by default.

Command mode: Admin Mode

2.2.4 traceroute

Command: traceroute {<*ip-addr*> | host <*hostname*> }[hops <*hops*>] [timeout <*timeout*>]

Function: This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed

sector.

Parameter: <*ip-addr*> is the target host IP address in dot decimal format. **<*hostname*>** is the hostname for the remote host. **<*hops*>** is the maximum gateway number allowed by Traceroute command. **<*timeout*>** Is the timeout value for test packets in milliseconds, between 100 – 10000.

Default: The default maximum gateway number is 16, timeout in 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

Related command: ip host

2.2.5 show

show command is used to display information about the system , port and protocol operation. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

2.2.5.1 show calendar

Command: show calendar

Function: Display the system clock.

Command mode: Admin Mode

Usage Guide: The user can use this command to check system date and time so that the system clock can be adjusted in time if inaccuracy occurs.

Example:

Switch#show calendar

Current time is TUE AUG 22 11: 00: 01 2002

Related command: calendar set

2.2.5.2 show debugging

Command: show debugging

Function: Display the debug switch status.

Usage Guide: If the user need to check what debug switches have been enabled, **show debugging** command can be executed.

Command mode: Admin Mode

Example: Check for currently enabled debug switch.

Switch#show debugging

STP:

Stp input packet debugging is on

Stp output packet debugging is on

Stp basic debugging is on

Switch#

Related command: debug

2.2.5.3 dir

Command: dir

Function: Display the files and their sizes in the Flash memory.

Command mode: Admin Mode

Example: Check for files and their sizes in the Flash memory.

Switch#dir

boot.rom	329,828 1900-01-01 00: 00: 00 --SH
boot.conf	94 1900-01-01 00: 00: 00 --SH
nos.img	2,449,496 1980-01-01 00: 01: 06 ----
startup-config	2,064 1980-01-01 00: 30: 12 ----

2.2.5.4 show history

Command: show history

Function: Display the recent user command history,.

Command mode: Admin Mode

Usage Guide: The system holds up to 10 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

Switch#show history

enable

config

interface ethernet 1/3

enable

dir

show ftp

2.2.5.5 show memory

Command: show memory

Function: Display the contents in the memory.

Command mode: Admin Mode

Usage Guide: This command is used for switch debug purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts: address, Hex view of the information and character view.

Example:

Switch#show memory
start address : 0x2100
number of words[64]:

002100: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002110: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002120: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002130: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002140: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002150: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002160: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*
002170: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

2.2.5.6 show running-config

Command: show running-config

Function: Display the current active configuration parameters for the switch.

Default: If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters.

Example:

Switch#show running-config

2.2.5.7 show startup-config

Command: show startup-config

Function: Display the switch parameter configurations written into the Flash memory at the current operation, those are usually also the configuration files used for the next power-up.

Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

2.2.5.8 show interfaces switchport

Command: show interfaces switchport [ethernet <interface >]

Function: Display VLAN interface mode and VLAN number, and Trunk port information for the switch.

Parameter: <*interface* > is the port number, which can be any port information exist in the switch.

Command mode: Admin Mode

Example: Display the VLAN information for interface ethernet 1/1.

Switch#show interfaces swichport ethernet 1/1
Ethernet1/1

Type : Universal
Mac addr num : -1
Mode : Access

Port VID : 1
Trunk allowed Vlan : ALL

Displayed information	Description
Ethernet1/1	Corresponding Ethernet interface number;
Type	Current Interface Type
Mac addr num	MAC address number can be learn by the current interface
Mode : Access	VLAN mode of the current Interface

Port VID : 1	VLAN number belong to the current Interface
Trunk allowed Vlan : ALL	VLAN allowed to be crossed by Trunk.

2.2.5.9 show tcp

Command: show tcp

Function: Display the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show tcp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local pot number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

2.2.5.10 show udp

Command: show udp

Function: Display the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show udp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSED
0.0.0.0	123	0.0.0.0	0	CLOSED
0.0.0.0	1985	0.0.0.0	0	CLOSED

Displayed information	Description
LocalAddress	Local address of the udp connection.
LocalPort	Local pot number of the udp connection.
ForeignAddress	Remote address of the udp connection.
ForeignPort	Remote port number of the udp connection.
State	Current status of the udp connection.

2.2.5.11 show users

Command: show users

Function: Display all user information that can login the switch .

Usage Guide: This command can be used to check for all user information that can login the switch .

Example:

Switch#show users

User level havePasword

admin 0 1

Online user info: user ip login time(second) usertype

Switch#

Related command: username password、username access-level

2.2.5.12 show version

Command: show version<unit>

Parameter: where the range of unit is 1

Function: Display the switch version.

Default: The default value for <unit> is 1

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version. 。

Example:

Switch#show vers

ES4626 Device, Apr 14 2005 11: 19: 29

HardWare version is 2.0, SoftWare version packet is ES4626_1.1.0.0, BootRom version is ES4626_1.0.4

Copyright (C) 2001-2006 by Accton Technology Corporation..

All rights reserved.

Last reboot is cold reset

Uptime is 0 weeks, 0 days, 0 hours, 28 minutes

2.2.6 debug

All the protocols ES4626/ES4650 supports have their corresponding debug commands. The users can use the information from debug command for troubleshooting. Debug commands for their corresponding protocols will be introduced in the later chapters.

2.3 Configuring Switch IP Addresses

All Ethernet ports of ES4626/ES4650 is default to DataLink layer ports and perform layer 2 forwarding. VLAN interface represent a Layer 3 interface function , which can be assigned an IP address, which is also the IP address of the switch. All VLAN interface related configuration commands can be configured under VLAN Mode. ES4626/ES4650 provides three IP address configuration methods:

- ☞ Manual
- ☞ BootP
- ☞ DHCP

Manual configuration of IP address is assign an IP address manually for the switch.

In BootP/DHCP mode, the switch operates as a BootP/DHCP client, send broadcast packets of BootPRequest to the BootP/DHCP servers, and the BootP/DHCP servers assign the address on receiving the request. In addition, ES4626/ES4650 can act as a DHCP server, and dynamically assign network parameters such as IP addresses, gateway addresses and DNS server addresses to DHCP clients DHCP Server configuration is detailed in later chapters.

2.3.1Configuring Switch IP Addresses Task Sequence

1. Manual configuration
2. BootP configuration
3. DHCP configuration

1. Manual configuration

Command	Explanation
ip address *<ip_address>* *<mask>* [secondary]	Configure the VLAN interface IP address; the "**no ip address *<ip_address>* *<mask>***

no ip address <*ip_address*> <*mask*> [secondary]	**[secondary]"** command deletes VLAN interface IP address.

2. BootP configuration

Command	Explanation
ip address bootp **no ip address bootp**	Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP client function.

3.DHCP

Command	Explanation
ip address dhcp **no ip address dhcp**	Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp-client enable**" command disables the DHCP client function.

2.3.2 Commands for Configuring Switch IP Addresses

2.3.2.1 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Set the IP address and mask for the specified VLAN interface; the "**no ip address <*ip address*> <*mask*> [secondary]"** command deletes the specified IP address setting.

Parameter: <*ip-address*> is the IP address in dot decimal format; **<*mask*>** is the subnet mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Default: No IP address is configured upon switch shipment.

Command mode: VLAN Interface Mode

Usage Guide: A VLAN interface must be created first before the user can assign an IP address to the switch.

Example: Set 10.1.128.1/24 as the IP address of VLAN1 interface.

Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-If-Vlan1)#exit
Switch(Config)#
Related command: ip address bootp、ip address dhcp

2.3.2.2 ip address bootp

Command: ip address bootpno ip address bootp
Function: Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP client function and releases the IP address obtained in BootP .
Default: BootP client function is disabled by default.
Command mode: VLAN Interface Mode
Usage Guide: Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any 2 methods for obtaining IP address is not allowed. Note: To obtain IP address via DHCP, a DHCP server or a BootP server is required in the network.
Example: Get IP address through BootP.
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address bootp
Switch (Config-If-Vlan1)#exit
Switch (Config)#
Related command: ip address、ip address dhcp

2.3.2.3 ip address dhcp

Command: ip address dhcp
no ip address dhcp
Function: Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp -client enable**" command disables the DHCP client function and releases the IP address obtained in DHCP . Note: To obtain IP address via DHCP, a DHCP server is required in the network.
Default: DHCP client function is disabled by default.
Command mode: VLAN Interface Mode
Usage Guide: Obtaining IP address through DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining IP address is not allowed.
Example: Get IP address through DHCP.

Switch (Config)#interface vlan 1
Switch (Config-If-Vlan1)# ip address dhcp
Switch (Config-If-Vlan1)#exit
Switch (Config)#
Related command: ip address, ip address bootp

2.4 SNMP

2.4.1Introduction to SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol widely used in computer network management. SNMP is an evolving protocol. SNMP v1 [RFC1157] is the first version of SNMP which is adapted by vast numbers of manufacturers for its simplicity and easy implementation; SNMP v2c is an enhanced version of SNMP v1, which supports layered network management; SNMP v3 strengthens the security by adding USM (User-based Security Mode) and VACM (View-based Access Control Model).

SNMP protocol provides a simple way of exchange network management information between two points in the network. SNMP employs a polling mechanism of message query, and transmits messages through UDP (a connectionless transport layer protocol). Therefore it is well supported by the existing computer networks.

SNMP protocol employs a station-agent mode. There are two parts in this structure: NMS (Network Management Station) and Agent. NMS is the workstation on which SNMP client program is running. It is the core on the SNMP network management. Agent is the server software runs on the devices which need to be managed. NMS manages all the managed objects through Agents. The switch supports Agent function.

The communication between NMS and Agent functions in Client/Server mode by exchanging standard messages. NMS sends request and the Agent responds. There are seven types of SNMP message:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS sends queries to the Agent with Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request messages; and the Agent, upon receiving the

requests, replies with Get-Response message. On some special situations, like network device ports are on Up/Down status or the network topology changes, Agents can send Trap messages to NMS to inform the abnormal events. Besides, NMS can also be set to alert to some abnormal events by enabling RMON function. When alert events are triggered, Agents will send Trap messages or log the event according to the settings. Inform-Request is mainly used for inter-NMS communication in the layered network management.

USM ensures the transfer security by well-designed encryption and authentication. USM encrypts the messages according to the user typed password. This mechanism ensures that the messages can't be viewed on transmission. And USM authentication ensures that the messages can't be changed on transmission. USM employs DES-CBC cryptography. And HMAC-MD5 and HMAC-SHA are used for authentication.

VACM is used to classify the users' access permission. It puts the users with the same access permission in the same group. Users can't conduct the operation which is not authorized.

2.4.2Introduction to MIB

The network management information accessed by NMS is well defined and organized in a Management Information Base (MIB). MIB is pre-defined information which can be accessed by network management protocols. It is in layered and structured form. The pre-defined management information can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MID. Each MIB organizes all the available information with this tree structure. And each node on this tree contains an OID (Object Identifier) and a brief description about the node. OID is a set of integers divided by periods. It identifies the node and can be used to locate the node in a MID tree structure, shown in the figure below:

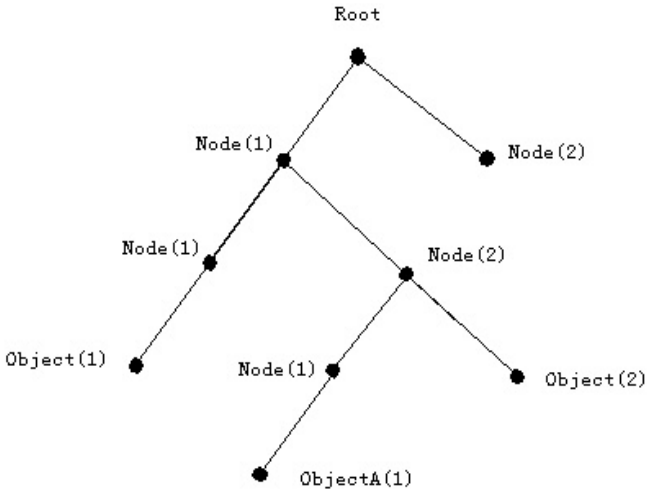


Fig 2-1 ASN.1 Tree Instance

In this figure, the OID of the object A is 1.2.1.1. NMS can locate this object through this unique OID and gets the standard variables of the object. MIB defines a set of standard variables for monitored network devices by following this structure.

If the variable information of Agent MIB needs to be browsed, the MIB browse software needs to be run on the NMS. MIB in the Agent usually consists of public MIB and private MIB. The public MIB contains public network management information that can be accessed by all NMS; private MIB contains specific information which can be viewed and controlled by the support of the manufacturers

MIB-I [RFC1156] is the first implemented public MIB of SNMP, and is replaced by MIB-II [RFC1213]. MIB-II expands MIB-I and keeps the OID of MIB tree in MIB-I. MIB-II contains sub-trees which are called groups. Objects in those groups cover all the functional domains in network management. NMS obtains the network management information by visiting the MIB of SNMP Agent.

The switch can operate as a SNMP Agent, and supports both SNMP v1/v2c and SNMP v3. The switch supports basic MIB-II, RMON public MIB and other public MID such as BRIDGE MIB. Besides, the switch supports self-defined private MIB.

2.4.3Introduction to RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used

group 1, 2, 3 and 9:

Statistics: Maintain basic usage and error statistics for each subnet monitored by the Agent.

History: Record periodical statistic samples available from Statistics.

Alarm: Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.

Event: A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

2.4.4SNMP Configuration

2.4.4.1 SNMP Configuration Task Sequence

1. Enable or disable SNMP Agent server function
2. Configure SNMP community string
3. Configure IP address of SNMP management base
4. Configure engine ID
5. Configure user
6. Configure group
7. Configure view
8. Configuring TRAP
9. Enable/Disable RMON

1. Enable or disable SNMP Agent server function

Command	Explanation
snmp-server **no snmp-server**	Enable the SNMP Agent function on the switch; the "**no snmp-server enable**" command disables the SNMP Agent function on the switch.

2. Configure SNMP community string

Command	Explanation
snmp-server community <*string*> {ro|rw} **no snmp-server community <*string*>**	Configure the community string for the switch; the "**no snmp-server community <*string*>**" command deletes the configured

	community string.

3. Configure IP address of SNMP management base

Command	Explanation
snmp-server securityip <*ip-address*> **no snmp-server securityip <*ip-address*>**	Configure the secure IP address which is allowed to access the switch on the NMS; the "**no snmp-server securityip <*ip-address*>**" command deletes configured secure address.
snmp-server SecurityIP enable **snmp-server SecurityIP disable**	Enable or disable secure IP address check function on the NMS.

4. Configure engine ID

Command	Explanation
snmp-server engineid < *engine-string* > **no snmp-server engineid < *engine-string* >**	Configure the local engine ID on the switch. This command is used for SNMP v3.

5. Configure user

Command	Explanation
snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}] **no snmp-server user <*user-string*> <*group-string*>**	Add a user to a SNMP group. This command is used to configure USM for SNMP v3.

6. Configure group

Command	Explanation
snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]] **no snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv}**	Set the group information on the switch. This command is used to configure VACM for SNMP v3.

7. Configure view

Command	Explanation
snmp-server view <*view-string*>	Configure view on the switch. This

<oid-string> **{include|exclude}** **no snmp-server view <*view-string*>**	command is used for SNMP v3.

8. Configuring TRAP

Command	Explanation
snmp-server enable traps **no snmp-server enable traps**	Enable the switch to send Trap message. This command is used for SNMP v1/v2/v3.
snmp-server host <*host-address* > {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*> **no snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*>**	Set the host IP address which is used to receive SNMP Trap information. For SNMP v1/v2, this command also configures Trap community string; for SNMP v3, this command also configures Trap user name and security level.

9. Enable/Disable RMON

Command	Explanation
rmon enable **no rmon enable**	Enable/disable RMON.

2.4.4.2 SNMP Configuration Commands

2.4.4.2.1 snmp-server

Command: snmp-server

no snmp-server

Function: Enable the SNMP agent server function on the switch; the "**no snmp-server enable"** command disables the SNMP agent server function**.**

Command mode: Global Mode

Default: SNMP agent server function is disabled by default.

Usage Guide: To enable configuration and management via network administrative software, this command must be executed to enable the SNMP agent server function on the switch.

Example: Enable SNMP Agent server function on the switch.

Switch(Config)#snmp-server

2.4.4.2.2 snmp-server community

Command: snmp-server community <*string*> {ro|rw}

nmp-server community <*string*>

Function: Configure the community string for the switch; the "**no snmp-server community <*string*>**" command deletes the configured community string.

Parameter: <*string*> is the community string set; **ro|rw** is the specified access mode to MIB, **ro** for read-only and **rw** for read-write.

Command mode: Global Mode

Usage Guide: The switch supports up to 4 community strings.

Example 1: Add a community string named "private" with read-write permission.

Switch(config)#snmp-server community private rw

Example 2: Add a community string named "public" with read-only permission.

Switch(config)#snmp-server community public ro

Example 3: Modify the read-write community string named "private" to read-only.

Switch(config)#snmp-server community private ro

Example 4: Delete community string "private".

Switch(config)#no snmp-server community private

2.4.4.2.3 snmp-server enable traps

Command: snmp-server enable traps

no snmp-server enable traps

Function: Enable the switch to send Trap message; the "**no snmp-server enable traps**" command disables the switch to send Trap message.

Command mode: Global Mode

Default: Trap message is disabled by default.

Usage Guide: When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

Example 1: Enable to send Trap messages.

Switch(config)#snmp-server enable traps

Example 2: Disable to send Trap messages.

Switch(config)#no snmp-server enable trap

2.4.4.2.4 snmp-server engineid

Command: snmp-server engineid < *engine-string* >

no snmp-server engineid

Function: Configure the engine ID; the "**no snmp-server engineid < engine-string >**" command restores the default engine ID.

Parameter: <engine-string> is the engine ID which is 1-32 hexadecimal characters.

Command mode: Global Mode

Default: The engine ID is manufacturer number + local MAC address by default.

Example 1: Set the engine ID to A66688999F.

Switch(config)#snmp-server engineid A66688999F

Example 2: Restore the default engine ID.

Switch(config)#no snmp-server engineid

2.4.4.2.5 snmp-server user

Command: snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}]

no snmp-server user <*user-string*> <*group-string*>

Function: Add a new user to SNMP group; The "**no snmp-server user <*user-string*> <*group-string*>**" command deletes the user.

Parameter: <user-string> is the user name which is 1 to 32 characters; **<group-string>** is the group name which the user belongs to; **encrypted** means that messages are encrypted by DES; **auth** means that messages are authenticated; **md5** is used for authentication; **sha** is used for authentication; **<password-string>** is user password which is 1 to 32 characters.

Command mode: Global Mode

Usage Guide: Messages are not encrypted by default. If users enable the encryption, they have to enable authentication. When users delete a user with the right user name and wrong group name, the user still can be deleted.

Example 1: Add a user named "tester" to group "UserGroup", with encryption, "HMAC md5" authentication and password "hello"

Switch (Config)#snmp-server user tester UserGroup encrypted auth md5 hello

Example 2: Delete a user.

Switch (Config)#no snmp-server user tester UserGroup

2.4.4.2.6 snmp-server group

Command: snmp-server group <group-string> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]]no

snmp-server group <group-string> {NoauthNopriv|AuthNopriv|AuthPriv}

Function: Configure a new SNMP server group; the "**no snmp-server group <group-string> {NoauthNopriv|AuthNopriv|AuthPriv}**" command deletes the group.

Parameter: <group-string > is the group name; **NoauthNopriv** means no encryption and no authentication; **AuthNopriv** means authentication and no encryption; **AuthPriv** means authentication and encryption; **read-string** is view name with read permission. It is 1 to 32 characters; **write-string** is view name with write permission. It is 1 to 32 characters; **notify-string** is view name with modify (trap) permission. It is 1 to 32 characters

Command mode: Global Mode

Usage Guide: There is a default view named "v1defaultviewname" which is recommended to be used. If there is no view with read or write permission, this operation is forbidden.

Example 1: Create a group named "CompanyGroup" with encryption and authentication. The view named "readview" with read permission but without write permission.

Switch (Config)#snmp-server group CompanyGroup AuthPriv read readview

Example 2: Delete the group.

Switch (Config)#no snmp-server group CompanyGroup AuthPriv

2.4.4.2.7 snmp-server view

Command: snmp-server view <*view-string*> <*oid-string*> {include|exclude}

no snmp-server view <*view-string*>

Function: Create or modify view information; the "**no snmp-server view <view-string>**" command deletes view information.

Parameter: < view-string > is the view name which is 1 to 32 characters; **< oid-string >** is OID string or the node name which is 1 to 255 characters. **include|exclude** refers to including or excluding the OID.

Command mode: Global Mode

Usage Guide: This command supports not only OID string but also node name.

Example 1: Create a view named "readview" which includes the node named "iso", but excludes the node named "iso.3"

Switch (Config)#snmp-server view readview iso include

Switch (Config)#snmp-server view readview iso.3 exclude

Example 2: Delete view.

Switch (Config)#no snmp-server view readview

2.4.4.2.8 snmp-server host

Command: snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*>

no snmp-server host <*host-address*> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} <*user-string*>

Function: This command functions differently for different versions of SNMP. For SNMP v1/v2, this command is used to configure Trap community string and the IP address of the NMS which receives SNMP Trap messages. For SNMP v3, this command is used to configure the IP address of the NMS which receives SNMP Trap messages, and Trap user name and security level; the "**no snmp-server host <host-address> {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} <user-string>**" command deletes the IP address.

Parameter: <*host-addr*> is the IP address of the NMS which receives SNMP Trap messages; **v1|v2c|v3** is SNMP version for Trap message; **NoauthNopriv|AuthNopriv|AuthPriv** is the security level: no authentication and no encryption **|** authentication and no encryption **|** authentication and encryption. <**user -*string*>** stands for the community string for sending Trap message for SNMP v1/v2; and it stands for user name for SNMP v3.

Command mode: Global Mode

Usage Guide: The community string in the command is also used for RMON event community string. If RMON event community string is not configured, the community string in the command is used for RMON event community string. If RMON event community string is configured, RMON event uses its own community string.

Example 1 : Set the IP address of the NMS which receives SNMP Trap messages.

Switch(config)#snmp-server host 1.1.1.5 v1 usertrap

Example 2 : Delete the IP address of the NMS which receives SNMP Trap messages.

Switch(config)#no snmp-server host 1.1.1.5 v1 usertrap

2.4.4.2.9 snmp-server securityip

Command: snmp-server securityip <*ip-address*>

no snmp-server securityip <*ip-address*>

Function: Configure the secure IP address which is allowed to access the switch on the NMS; the "**no snmp-server securityip <*ip-address*>**" command deletes configured secure address.

Parameter: <*ip-address*> is the secure IP address in dotted decimal format.

Command mode: Global Mode

Usage Guide: Only if the IP address of NMS and the secure IP address are the same, the SNMP messages sent by the NMS are processed by the switch. This command is only

used for SNMP v1 and SNMP v2.

Example 1: Set the secure IP address to 1.1.1.5

Switch(config)#snmp-server securityip 1.1.1.5

Example 2: Delete the secure IP address

Switch(config)#no snmp-server securityip 1.1.1.5

2.4.4.2.10 snmp-server SecurityIP enable

Command: snmp-server SecurityIP enable

snmp-server SecurityIP disable

Function: Enable or disable secure IP address check function on the NMS.

Command mode: Global Mode

Default: Secure IP address check function is enabled by default.

Example: Disable secure IP address check function.

Switch(config)#snmp-server securityip disable

2.4.4.2.11 rmon enable

Command: rmon enable

no rmon enable

Function: Enable RMON; the "**no rmon enable**" command disables RMON.

Command mode: Global Mode

Default: RMON is disabled by default.

Example 1: Enable RMON

Switch(config)#rmon enable

Example 2: Disable RMON

Switch(config)#no rmon enable

2.4.5Typical SNMP Configuration Examples

The IP address of the NMS is 1.1.1.5; the IP address of the switch (Agent) is 1.1.1.9

Scenario 1: The NMS network administrative software uses SNMP protocol to obtain data from the switch.

The configuration on the switch is listed below:

Switch(config)#snmp-server

Switch(Config)#snmp-server community private rw
Switch(Config)#snmp-server community public ro
Switch(Config)#snmp-server securityip 1.1.1.5

The NMS can use “private” as the community string to access the switch with read-write permission, or use “public” as the community string to access the switch with read-only permission.

Scenario 2: NMS will receive Trap messages from the switch (Note: NMS may have community string verification for the Trap messages. In this scenario, the NMS uses a Trap verification community string of “ectrap”).
The configuration on the switch is listed below:
Switch(config)#snmp-server
Switch(Config)#snmp-server host 1.1.1.5 ectrap
Switch(Config)#snmp-server enable traps

Scenario 3: NMS uses SNMP v3 to obtain information from the switch.
The configuration on the switch is listed below:
Switch(config)#snmp-server
Switch (Config)#snmp-server user tester UserGroup encrypted auth md5 hello
Switch (Config)#snmp-server group UserGroup AuthPriv read max write max notify max
Switch (Config)#snmp-server view max 1 include

Scenario 4: NMS wants to receive the v3Trap messages sent by the switch.
The configuration on the switch is listed below:
Switch(config)#snmp-server
Switch(config)#snmp-server host 10.1.1.2 v3 AuthPriv tester
Switch(config)#snmp-server enable traps

2.4.6SNMP Troubleshooting Help

2.4.6.1Monitor and Debug Commands

2.4.6.1.1 show snmp

Command: show snmp

Function: Display all SNMP counter information.

Command mode: Admin Mode

Example:

Switch#show snmp

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Max packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Get-response PDUs

0 SNMP trap PDUs

Displayed information	Explanation
snmp packets input	**Total number of SNMP packet inputs.**
bad snmp version errors	Number of version information error packets.
unknown community name	Number of community name error packets.
illegal operation for community name supplied	Number of permission for community name error packets.
encoding errors	Number of encoding error packets.
number of requested variablest	Number of variables requested by NMS.
number of altered variables	Number of variables set by NMS.
get-request PDUs	Number of packets received by “get” requests.
get-next PDUs	Number of packets received by “getnext” requests.
set-request PDUs	Number of packets received by “set” requests.

snmp packets output	Total number of SNMP packet outputs.
too big errors	Number of “Too_ big” error SNMP packets.
maximum packet size	Maximum length of SNMP packets.
no such name errors	Number of packets requesting for non-existent MIB objects.
bad values errors	Number of “Bad_values” error SNMP packets.
general errors	Number of “General_errors” error SNMP packets.
response PDUs	Number of response packets sent.
trap PDUs	Number of Trap packets sent.

2.4.6.1.2 show snmp status

Command: show snmp status

Function: Display SNMP configuration information.

Command mode: Admin Mode

Example:

Switch#show snmp status

Trap enable

RMON enable

Community Information:

V1/V2c Trap Host Information:

V3 Trap Host Information:

Security IP Information:

Displayed information	Description
Community string	Community string
Community access	Community access permission
Trap-rec-address	IP address which is used to receive Trap.
Trap enable	Enable or disable to send Trap.
SecurityIP	IP address of the NMS which is allowed to access Agent

2.4.6.1.3 show snmp engineid

Command: show snmp engineid

Function: Display SNMP engine ID information.

Command mode: Admin Mode

Example:

Switch#show snmp engineid

SNMP engineID: 3138633303f1276c Engine Boots is: 1

Displayed information	Description
SNMP engineID	SNMP engine ID
Engine Boots	The number of times that the engine boots.

2.4.6.1.4 show snmp user

Command: show snmp user

Function: Display user name information.

Command mode: Admin Mode

Example:

Switch#show snmp user

User name: initialsha

Engine ID: 1234567890

Auth Protocol: MD5 Priv Protocol: DES-CBC

Row status: active

Displayed information	Description
User name	User name
Engine ID	Engine ID
Priv Protocol	Encryption protocol
Auth Protocol	Authentication protocol
Row status	User state

2.4.6.1.5 show snmp group

Command: show snmp group

Function: Display group information.

Command mode: Admin Mode

Example:

Switch#show snmp group

Group Name: initial Security Level: noAuthnoPriv

Read View: one

Write View: <no writeview specified>

Notify View: one

Displayed information	Description
Group Name	Group name
Security level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	Users don't specify view names.

2.4.6.1.6 show snmp view

Command: show snmp view

Function: Display view information.

Command mode: Admin Mode

Example:

Switch#show snmp view

View Name: readview 1. -Included active

1.3. - Excluded active

Displayed information	Description
View Name	View name
1. and 1.3.	OID number
Included	View includes the sub-tree which has this OID as the root.
Excluded	View doesn't include the sub-tree which has this OID as the root.
active	State

2.4.6.1.7 show snmp mib

Command: show snmp mib

Function: Display all the MIB supported on the switch.

Command mode: Admin Mode

2.4.6.2SNMP Troubleshooting Help

When users configure the SNMP, the SNMP server may fail to run properly due to physical connection failure and wrong configuration, etc. Users can troubleshoot the problems by following the guide below:

- ✧ Good condition of the physical connection.
- ✧ Interface and datalink layer protocol is Up (use the “show interface” command), and the connection between the switch and host can be verified by ping (use “ping” command).
- ✧ The switch enabled SNMP Agent server function (use “snmp-server” command)
- ✧ Secure IP for NMS (use “snmp-server securityip” command) and community string (use “snmp-server community” command) are correctly configured, as any of them fails, SNMP will not be able to communicate with NMS properly.
- ✧ If Trap function is required, remember to enable Trap (use “snmp-server enable traps” command): Qnd remember to properly configure the target host IP address and community string for Trap (use “snmp-server host” command) to ensure Trap message can be sent to the specified host.
- ✧ If RMON function is required, RMON must be enabled first (use “rmon enable” command).
- ✧ Use “show snmp” command to verify sent and received SNMP messages; Use “show snmp status” command to SNMP configuration information; Use “debug snmp packet” to enable SNMP debug function and verify debug information.
- ✧ If users still can’t solve the SNMP problems, Please contact our technical and service center.

2.5 Switch Upgrade

ES4626/ES4650 provides two ways for switch upgrade: BootROM upgrade and the TFTP/FTP upgrade under Shell.

2.5.1 BootROM Upgrade

There are two methods for BootROM upgrade: TFTP and FTP, which can be selected at BootROM command settings.

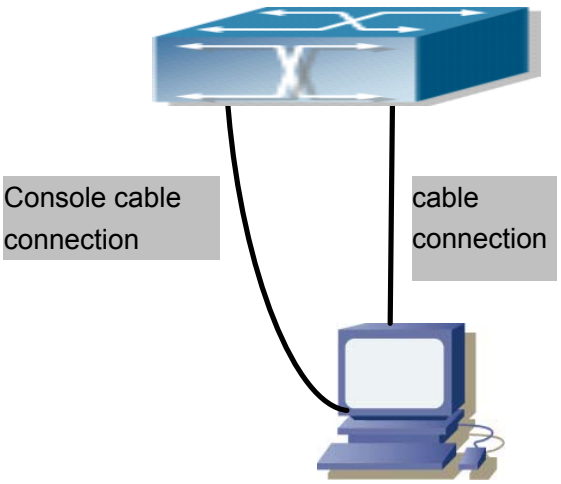


Fig -2-2 Typical topology for switch upgrade in BootROM mode

The upgrade procedures are listed below:

Step 1:

As shown in the figure, a PC is used as the console for the switch. A console cable is used to connect PC to the management port on the switch. The PC should have FTP/TFTP server software installed and has the img file required for the upgrade.

Step 2:

Press “ctrl+b” on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below:

ES4626 Management Switch

Copyright (c) 2001-2004 by Accton Technology Corporation.
All rights reserved.

Reset chassis ... done.
Testing RAM...
134,217,728 RAM OK.

Loading BootROM...
Starting BootRom...
Attaching to file system ... done.
265.96 BogoMIPS
CPU: Motorola MPC82xx ADS - HIP7
Version: 5.4

BootRom version: 1.0.4
Creation date: Jun 9 2006, 14: 54: 12

Attached TCP/IP interface to lnPci0.
[Boot]:

Step 3:

Under BootROM mode, run “setconfig” to set the IP address and mask of the switch under BootROM mode, server IP address and mask, and select TFTP or FTP upgrade. Suppose the switch address is 192.168.1.2/24, and PC address is 192.168.1.66/24, and select TFTP upgrade, the configuration should like:

[Boot]: setconfig
Host IP Address: 10.1.1.1 192.168.1.2
Server IP Address: 10.1.1.2 192.168.1.66
FTP(1) or TFTP(2): 1 2
Network interface configure OK.
[Boot]:

Step 4:

Enable FTP/TFTP server in the PC. For TFTP, run TFTP server program; for FTP, run FTP server program. Before start downloading upgrade file to the switch, verify the connectivity between the server and the switch by ping from the server. If ping succeeds, run “load” command in the BootROM mode from the switch; if it fails, perform troubleshooting to find out the cause. The following is the configuration for the system update mirror file.

[Boot]: load nos.img
Loading...
entry = 0x10010
size = 0x1077f8

Step 5:

Execute “write nos.img” in BootROM mode. The following saves the system update mirror file.

[Boot]: write nos.img
Programming...

Program OK.

[Boot]:

Step 6:

After successful upgrade, execute “run” command in BootROM mode to return to CLI configuration interface.

[Boot]: run（or reboot）

Other commands in BootROM mode

1. DIR command

Used to list existing files in the FLASH.

[Boot]: dir

boot.rom 327,440 1900-01-01 00: 00: 00 --SH
boot.conf 83 1900-01-01 00: 00: 00 --SH
nos.img 2,431,631 1980-01-01 00: 21: 34 ----
startup-config 2,922 1980-01-01 00: 09: 14 ----
temp.img 2,431,631 1980-01-01 00: 00: 32 ----

2. CONFIG RUN command

Used to set the IMG file to run upon system start-up, and the configuration file to run upon configuration recovery.

[Boot]: config run

Boot File: [nos.img] nos1.img

Config File: [boot.conf]

2.5.2 FTP/TFTP Upgrade

2.5.2.1 Introduction to FTP/TFTP

FTP(File Transfer Protocol)/TFTP(Trivial File Transfer Protocol) are both file transfer protocols that belonging to fourth layer(application layer) of the TCP/IP protocol stack, used for transferring files between hosts, hosts and switches. Both of them transfer files in a client-server model. Their differences are listed below.

FTP builds upon TCP to provide reliable connection-oriented data stream transfer service. However, it does not provide file access authorization and uses simple authentication mechanism(transfers username and password in plain text for authentication). When using FTP to transfer files, two connections need to be established between the client and the server: a management connection and a data connection. A transfer request should be sent by the FTP client to establish management connection on port 21 in the server, and negotiate a data connection through the management connection.

There are two types of data connections: active connection and passive connection.

In active connection, the client transmits its address and port number for data transmission to the sever, the management connection maintains until data transfer is complete. Then, using the address and port number provided by the client, the server establishes data connection on port 20 (if not engaged) to transfer data; if port 20 is engaged, the server automatically generates some other port number to establish data connection.

In passive connection, the client, through management connection, notify the server to establish a passive connection. The server then create its own data listening port and inform the client about the port, and the client establishes data connection to the specified port.

As data connection is established through the specified address and port, there is a third party to provide data connection service.

TFTP builds upon UDP, providing unreliable data stream transfer service with no user authentication or permission-based file access authorization. It ensures correct data transmission by sending and acknowledging mechanism and retransmission of time-out packets. The advantage of TFTP over FTP is that it is a simple and low overhead file transfer service.

ES4626/ES4650 can operate as either FTP/TFTP client or server. When ES4626/ES4650 operates as a FTP/TFTP client, configuration files or system files can be downloaded from the remote FTP/TFTP servers(can be hosts or other switches) without affecting its normal operation. And file list can also be retrieved from the server in ftp client mode. Of course, ES4626/ES4650 can also upload current configuration files or system files to the remote FTP/TFTP servers(can be hosts or other switches). When ES4626/ES4650 operates as a FTP/TFTP server, it can provide file upload and download service for authorized FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

ROM: Short for EPROM, erasable read-only memory. EPROM is repalced by FLASH memory in ES4626/ES4650.

SDRAM: RAM memory in the switch, used for system software operation and configuration sequence storage.

FLASH: Flash memory used to save system file and configuration file

System file: including system mirror file and boot file.

System mirror file: refers to the compressed file for switch hardware driver and software support program, usually refer to as IMG upgrade file. In ES4626/ES4650, the system mirror file is allowed to save in FLASH only. ES4626/ES4650 mandates the name of system mirror file to be uploaded via FTP in Global Mode to be nos.img, other IMG system files will be rejected.

Boot file: refers to the file initializes the switch, also referred to as the ROM upgrade file (Large size file can be compressed as IMG file). In ES4626/ES4650, the boot file is

allowed to save in ROM only. ES4626/ES4650 mandates the name of the boot file to be boot.rom.

Configuration file: including start up configuration file and active configuration file. The distinction between start up configuration file and active configuration file can facilitate the backup and update of the configurations.

Start up configuration file: refers to the configuration sequence used in switch start up. ES4626/ES4650 start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, ES4626/ES4650 mandates the name of start up configuration file to be startup-config.

Active configuration file: refers to the active configuration sequence use in the switch. In ES4626/ES4650, the active configuration file stores in the RAM. In the current version, the active configuration sequence running-config can be saved from the RAM to FLASH by **write** command or **copy running-config startup-config** command, so that the active configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, ES4626/ES4650 mandates the name of active configuration file to be running-config.

Factory configuration file: The configuration file shipped with ES4626/ES4650 in the name of factory-config. Run **set default** and **write**, and restart the switch, factory configuration file will be loaded to overwrite current start up configuration file.

2.5.2.2 FTP/TFTP Configuration

The configurations of ES4626/ES4650 as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

2.5.2.2.1 FTP/TFTP Configuration Task Sequence

1. FTP/TFTP client configuration

Upload/download the configuration file or system file.

（1） For FTP client, server file list can be checked.

2. FTP server configuration

（1）Start FTP server

（2）Configure FTP login username and password

（3）Modify FTP server connection idle time

（4）Shut down FTP server

3. TFTP server configuration

（1）Start TFTP server

（2）Configure TFTP server connection idle time

（3）Configure retransmission times before timeout for packets without acknowledgement

（4）Shut down TFTP server

1. FTP/TFTP client configuration

（1）FTP/TFTP client upload/download file

Command	Explanation
Admin Mode	
copy <*source-url*> <*destination-url*> [ascii | binary]	FTP/TFTP client upload/download file

（2）For FTP client, server file list can be checked.

Global Mode	
dir <*ftpServerUrl*>	For FTP client, server file list can be checked. *FtpServerUrl* format looks like: ftp: //user: password@IP Address

2. FTP server configuration

（1）Start FTP server

Command	Explanation
Global Mode	
ftp-server enable **no ftp-server enable**	Start FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

（2）Modify FTP server connection idle time

Command	Explanation
Global Mode	
ftp-server timeout <*seconds*>	Set connection idle time

3. TFTP server configuration

（1）Start TFTP server

Command	Explanation
Global Mode	
tftp-server enable **no tftp-server enable**	Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

（2）Modify TFTP server connection idle time

Command	Explanation
Global Mode	
tftp-server retransmission-number < ***number*** **>**	Set maximum retransmission time within timeout interval.

（3）Modify TFTP server connection retransmission time

Command	Explanation
Global Mode	
tftp-server retransmission-number < ***number*** **>**	Set maximum retransmission time within timeout interval.

2.5.2.2.2 FTP/TFTP Configuration Commands

2.5.2.2.3 copy（FTP）

Command: copy <*source-url*> <*destination-url*> [ascii | binary]

Function: FTP client upload/download file

Parameter: <***source-url***> is the source file or directory location to be copied; **<*destination-url*>** is the target address to copy file or directory; <***source-url***> and **<*destination-url*>** varies according to the file or directory location. **ascii** Indicates the files are transferred in ASCII; **binary** indicates the files are transferred in binary (default) The URL format for FTP address looks like:

ftp: //<*username*>: <*password*>@<*ipaddress*>/<*filename*>, where <*username*>

is the FTP username, <*password*> is the FTP user password, <*ipaddress*> is the IP address of FTP server/client; <*filename*> is the name of the file to be uploaded/downloaded via FTP.

Special Keywords in filename

keyword	**Source/Target IP address**
running-config	Active configuration file
startup-config	Start up configuration file
nos.img	System file
boot.rom	System boot file

Command mode: Admin Mode

Usage Guide: The command provides command line prompt messages. If the user enters a command like **copy *<filename>* ftp: //** or **copy ftp: // *<filename>*** and press Enter, the following prompt will appear:

ftp server ip address [x.x.x.x] :

ftp username>

ftp password>

ftp filename>

This prompts for the FTP server address, username, password and file name.

Example:

（1）Save the mirror in FLASH to FTP server 10.1.1.1, the login username for the FTP server is “Switch”, and the password is “Accton”.

Switch#copy nos.img ftp: //Switch: Accton@10.1.1.1/nos.img

（2）Get the system file nos.img from FTP server 10.1.1.1, the login username for the FTP server is “Switch”, and the password is “Accton”.

Switch#copy ftp: //Switch: sAccton@10.1.1.1/nos.img nos.img

（3）Save active configuration file:

Switch#copy running-config startup-config

Related command: write

2.5.2.2.4 dir

Command: dir <ftp-server-url>

Function: check the list for files in the FTP server

Parameter: < *ftp-server-url* > takes the following format: ftp: //<*username*>: <*password*>@<*ipaddress*>, where <*username*> is the FTP username, <*password*> is the FTP user password, <*ipaddress*> is the IP address of FTP server.

Command mode: Global Mode

Example: view file list of the FTP server 10.1.1.1 with the username “Switch” and password “switch”.

Switch#config

Switch(Config)#dir ftp: //Switch: switch@10.1.1.1

2.5.2.2.5 ftp-server enable

Command: ftp-server enable

no ftp-server enable

Function: Start FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

Default: FTP server is not started by default.

Command mode: Global Mode

Usage Guide: When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not started by default.

Example: enable FTP server service.

Switch#config

Switch(Config)# ftp-server enable

2.5.2.2.6 ftp-server timeout

Command: ftp-server timeout <*seconds*>

Function: Set data connection idle time

Parameter: < *seconds*> is the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600.

Default: The system default is 600 seconds.

Command mode: Global Mode

Usage Guide: When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.

Example: Modify the idle threshold to 100 seconds.

Switch#config

Switch(Config)#ftp-server timeout 100

2.5.2.2.7 copy（TFTP）

Command: copy <source-url> <destination-url> [ascii | binary]

Function: TFTP client upload/download file

Parameter: <*source-url*> is the source file or directory location to be copied; <*destination-url*> is the target address to copy file or directory; <*source-url*> and <*destination-url*> varies according to the file or directory location. ascii Indicates the files are transferred in ASCII; binary indicates the files are transferred in binary (default) The URL format for TFTP address looks like: tftp: //<*ipaddress*>/<*filename*>, where <*ipaddress*> is the IP address of TFTP server/client, <*filename*> is the name of the file to be uploaded/downloaded via TFTP.

Special Keywords in filename

keyword	Source/Target IP address
running-config	Active configuration file
startup-config	Start up configuration file
nos.img	System file
boot.rom	System boot file

Command mode: Admin Mode

Usage Guide: The command provides command line prompt messages. If the user enters a command like copy <*filename*> tftp: // or copy tftp: // <*filename*> and press Enter, the following prompt will appear:

tftp server ip address>

tftp filename>

This prompts for the TFTP server address and file name.

Example:

（1）Save the mirror in FLASH to TFTP server 10.1.1.1:

Switch#copy nos.img tftp: // 10.1.1.1/ nos.img

（2）Get the system file nos.img from TFTP server 10.1.1.1:

Switch#copy tftp: //10.1.1.1/nos.img nos.img

（3）Save active configuration file:

Switch#copy running-config startup-config

Related command: write

2.5.2.2.8 tftp-server enable

Command: tftp-server enable

no tftp-server enable

Function: Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

Default: TFTP server is not started by default.

Command mode: Global Mode

Usage Guide: When TFTP server function is enabled, the switch can still perform tftp client functions. TFTP server is not started by default.

Example: enable TFTP server service.

Switch#config

Switch(Config)#tftp-server enable

Related command: tftp-server timeout

2.5.2.2.9 tftp-server retransmission-number

Command: tftp-server retransmission-number <*number*>

Function: Set the retransmission time for TFTP server

Parameter: < *number*> is the time to re-transfer, the valid range is 1 to 20.

Default: The default value is 5 retransmission.

Command mode: Global Mode

Example: Modify the retransmission to 10 times.

Switch#config

Switch(Config)#tftp-server retransmission-number 10

2.5.2.2.10 tftp-server transmission-timeout

Command: tftp-server transmission-timeout <*seconds*>

Function: Set the transmission timeout value for TFTP server

Parameter: < *seconds*> is the timeout value, the valid range is 5 to 3600s.

Default: The system default timeout setting is 600 seconds.

Command mode: Global Mode

Example: Modify the timeout value to 60 seconds.

Switch#config

Switch(Config)#tftp-server transmission-timeout 60

2.5.2.3 FTP/TFTP Configuration Examples

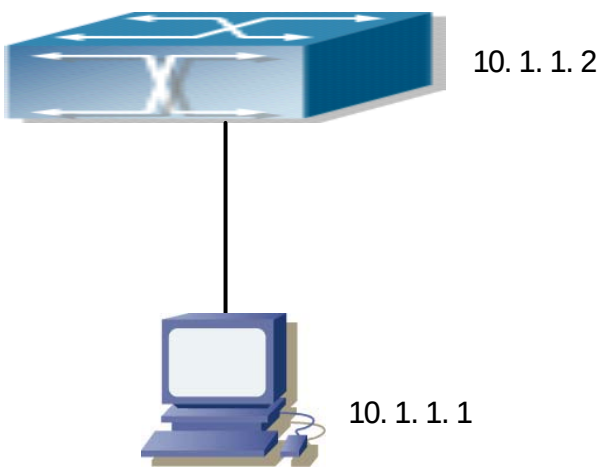


Fig -2-3 Download nos.img file as FTP/TFTP client

Scenario 1: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; the switch acts as a FTP/TFTP client, the IP address of the switch management VLAN is 10.1.1.2. Download “nos.img” file in the computer to the switch.

- **FTP Configuration**

Computer side configuration:

Start the FTP server software on the computer and set the username “Switch”, and the password “switch”. Place the “12_30_nos.img” file to the appropriate FTP server directory on the computer.

The configuration procedures of the switch is listed below:

```
Switch(Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy ftp: //Switch: Admin@10.1.1.1/12_30_nos.img nos.img
```

With the above commands, the switch will have the “nos.img” file in the computer downloaded to the FLASH.

- **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place the “nos.img” file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch is listed below:

```
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy tftp: //10.1.1.1/12_30_nos.img nos.img
```

Scenario 2: The switch is used as FTP server. The switch operates as the FTP server and connects from one of its ports to a computer, which is a FTP client. Transfer the “nos.img” file in the switch to the computer and save as 12_25_nos.img.

The configuration procedures of the switch is listed below:

```
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
```

Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#ftp-server enable
Switch(Config)# username Switch password 0 Admin

Computer side configuration:
Login to the switch with any FTP client software, with the username “Admin” and password “switch”, use the command “get nos.img 12_25_nos.img” to download “nos.img” file from the switch to the computer.

Scenario 3: The switch is used as TFTP server. The switch operates as the TFTP server and connects from one of its ports to a computer, which is a TFTP client. Transfer the “nos.img” file in the switch to the computer.
The configuration procedures of the switch is listed below:
Switch(Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#tftp-server enable
Computer side configuration:
Login to the switch with any TFTP client software, use the “tftp” command to download “nos.img” file from the switch to the computer.

Scenario 4: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; several switch user profile configuration files are saved in the computer. The switch operates as the FTP/TFTP client, the management VLAN IP address is 10.1.1.2. Download switch user profile configuration files from the computer to the switch FLASH.

- **FTP Configuration**

Computer side configuration:
Start the FTP server software on the computer and set the username “Switch”, and the password “Admin”. Save “Profile1”, “Profile2” and “Profile3” in the appropriate FTP server directory on the computer.
The configuration procedures of the switch is listed below:
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy ftp: //Switch: Admin@10.1.1.1/Profile1 Profile1
Switch#copy ftp: //Switch: Admin@10.1.1.1/Profile2 Profile2
Switch#copy ftp: //Switch: Admin@10.1.1.1/Profile3 Profile3
With the above commands, the switch will have the user profile configuration file in the computer downloaded to the FLASH.

- **TFTP Configuration**

Computer side configuration:
Start TFTP server software on the computer and place “Profile1”, “Profile2” and “Profile3” to the appropriate TFTP server directory on the computer.
The configuration procedures of the switch is listed below:
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy tftp: //10.1.1.1/ Profile1 Profile1
Switch#copy tftp: //10.1.1.1/ Profile2 Profile2
Switch#copy tftp: //10.1.1.1/ Profile3 Profile3

Scenario 5: ES4626/ES4650 acts as FTP client to view file list on the FTP server.
Synchronization conditions: The switch connects to a computer by a Ethernet port, the computer is a FTP server with an IP address of 10.1.1.1; the switch acts as a FTP client, and the IP address of the switch management VLAN1 interface is 10.1.1.2.

FTP Configuration

PC side:
Start the FTP server software on the PC and set the username “Switch”, and the password “Admin”.
ES4626:
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#dir ftp: //Switch: Admin@10.1.1.1
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.

230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
shell maintenance statistics.xls
… (some display omitted here)
show.txt
snmp.TXT
226 Transfer complete.
Switch (Config)#

2.5.2.4 FTP/TFTP Troubleshooting Help

2.5.2.4.1 Monitor and Debug Commands

2.5.2.4.1.1 show ftp

Command: show ftp
Function: display the parameter settings for the FTP server
Command mode: Admin Mode
Default: No display by default.
Example:
Switch#show ftp
Timeout : 600

Displayed information	Description
Timeout	Timeout time.

2.5.2.4.1.2 show tftp

Command: show tftp
Function: display the parameter settings for the TFTP server

Default: No display by default.

Command mode: Admin Mode

Example:

Switch#show tftp

timeout : 60

Retry Times : 10

Displayed information	Explanation
Timeout	Timeout time.
Retry Times	Retransmission times.

2.5.2.4.2 FTP Troubleshooting Help

When upload/download system file with FTP protocol, the connectivity of the link must be ensured, i.e., use the "**Ping**" command to verify the connectivity between the FTP client and server before running the FTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

☞ The following is what the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry "copy" command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...

331 User name okay, need password.

230 User logged in, proceed.

200 PORT Command successful.

nos.img file length = 1526021

read file ok

send file

150 Opening ASCII mode data connection for nos.img.

226 Transfer complete.

close ftp client.

☞ The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry "copy" command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...

331 User name okay, need password.

230 User logged in, proceed.

200 PORT Command successful.

recv total = 1526037

****

write ok

150 Opening ASCII mode data connection for nos.img (1526037 bytes).

226 Transfer complete.

- ☞ If the switch is upgrading system file or system start up file through FTP, the switch must not be restarted until “close ftp client” or “226 Transfer complete.” is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through FTP fails, please try to upgrade again or use the BootROM mode to upgrade.

2.5.2.4.3 TFTP Troubleshooting Help

When upload/download system file with TFTP protocol, the connectivity of the link must be ensured, i.e., use the “**Ping**” command to verify the connectivity between the TFTP client and server before running the TFTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

- ☞ The following is the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry “copy” command again.

  nos.img file length = 1526021

  read file ok

  begin to send file,wait...

  file transfers complete.

  close tftp client.

- ☞ The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry “copy” command again.

  begin to receive file,wait...

  recv 1526037

  ****

  write ok

  transfer complete

  close tftp client.

If the switch is upgrading system file or system start up file through TFTP, the switch must not be restarted until “close tftp client” is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through TFTP fails, please try upgrade again or use the BootROM mode to upgrade.

2.6 WEB Management

Click Switch Basic Configuration. Users can deploy the switch basic configuration such as enter or quit privileged mode, enter or quit interface mode, show switch clock and show switch system version etc.

2.6.1 Switch Basic Configuration

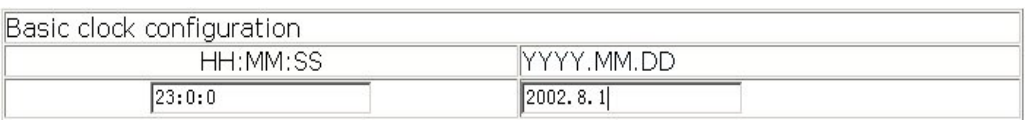
Click Switch Basic Configuration, Switch Basic Configuration. Users can configure switch clock, CLI prompt message and timeout value for exiting Admin Mode etc.

2.6.1.1BasicConfig

Click Switch Basic Configuration, Switch Basic Configuration, BasicConfig. Users can configure switch clock, CLI prompt message and mapping between hosts and IP addresses.

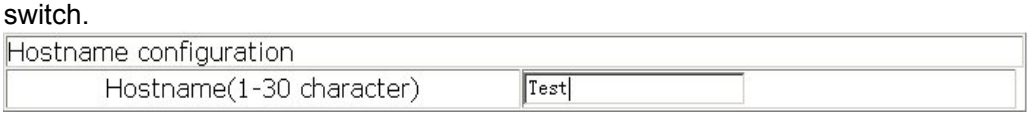
- ☞ Basic clock configuration - Configure system date and clock. See the equivalent CLI command at 2.1.1

Set HH: MM: SS to 23: 0: 0, set YY.MM.DD to 2002.8.1, and then click Apply. The switch time is set.



- ☞ Hostname configuration - Configure switch CLI prompt message. See the equivalent CLI command at 2.1.9

Set Hostname to Test, and then click Apply. The configuration is applied on the switch.



2.6.1.2Configure exec timeout

Click Switch Basic Configuration, Switch Basic Configuration, Configure exec timeout. Configure timeout value for exiting Admin Mode. See the equivalent CLI command at 2.1.5

Set Timeout to 6, and then click Apply. The switch timeout value for exiting Admin Mode is set to 6 minutes.



2.6.2SNMP Configuration

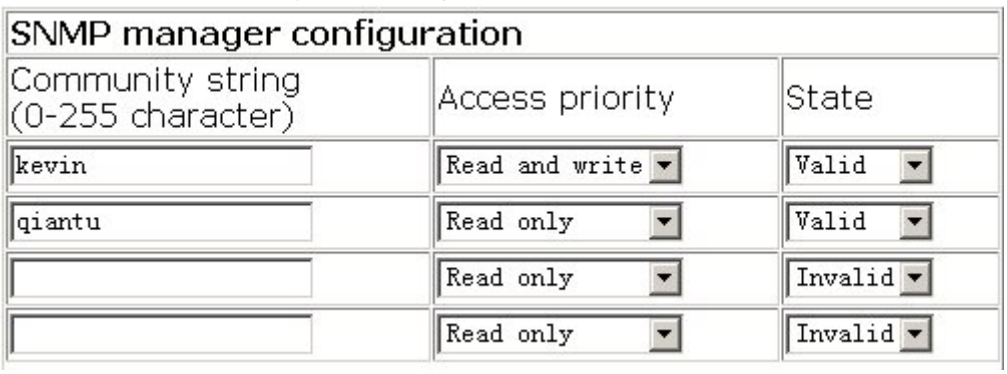
Click Switch Basic Configuration, SNMP Configuration. The switch SNMP configuration is shown. Users can configure SNMP.

2.6.2.1 SNMP manager configuration

Click Switch Basic Configuration, SNMP Configuration, SNMP manager configuration. Configure switch community string. See the equivalent CLI command at 2.4.4.2.2

- Community string (0-255 character) - Configure community string
- Access priority - Specify access mode to MIB. There are two options: Read only and Read and write.
- State - Valid means to set; Invalid means to delete

For example: Set Community string to qiantu; set Access priority to Read only; set State to Valid, and click Apply. The configuration is applied on the switch.



2.6.2.2 TRAP manager configuration

Click Switch Basic Configuration, SNMP Configuration, TRAP manager configuration. Users can configure the IP address and Trap community string of the NMS to receive SNMP trap message. See the equivalent CLI command at 2.4.4.2.5

- Trap receiver - IP address of NMS to receive Trap messages
- Community string (0-255 character) - Community string used in sending Trap message
- State - Valid means to set; Invalid means to delete

For example: Set Trap receiver to 41.1.100, set Community string to kevin, set State to Valid, and then click Apply. The configuration is applied on the switch.

TRAP manager configuration		
Trap receiver	Community string (0-255 character)	State
41.1.1.100	kevin	Valid
		Invalid
		Invalid
		Invalid

2.6.2.3 Configure ip address of snmp manager

Click Switch Basic Configuration, SNMP Configuration. Users can configure the secure IP address for NMS allowed to access the switch. See the equivalent CLI command at 2.4.4.2.6

- Security ip address - NMS secure IP address
- State - Valid means to set; Invalid means to delete

For example: Set Security ip address to 41.1.1.100, set State to Valid, and then click Apply. The configuration is applied on the switch.

Configure ip address of snmp manager	
Security ip address	State
41.1.1.100	Valid
	Invalid
	Invalid
	Invalid
	Invalid
	Invalid

2.6.2.4 SNMP statistics

Click Switch Basic Configuration, SNMP Configuration, SNMP statistics. Users can display SNMP configuration information. See the equivalent CLI command at 2.4.6.1.1.

SNMP statistics	number		SNMP statistics	Number
incoming snmp packet	0		Version error snmp packet	0
Received snmp getNext packet	0		Received SET request packet	0
outgoing snmp packet	0		too_big error snmp packet	0
Max-Length of snmp datagram	1500		snmp request for inexistent MIB object	0
Bad_value error snmp packet	0		General_error snmp packet	0
Transmitting response packet	0		Transmitting TRAP packet	0
Nms SET request packet	0		Nms SET request packet	0
Communitry string error snmp packet	0		Communitry string priority error	0
Coding error snmp packet	0			

2.6.2.5 RMON and TRAP configuration

Click Switch Basic Configuration, SNMP Configuration, RMON and TRAP configuration. Users can configure switch RMON:

- ☞ Snmp Agent state - Enable/disable the switch as SNMP agent. See the equivalent CLI command at 2.4.4.2.3
- ☞ RMON state - Enable/disable RMON on the switch. See the equivalent CLI command at 2.4.4.2.1
- ☞ Trap state - Enable the switch to send Trap messages. See the equivalent CLI command at 2.4.4.2.4

For example: Set Snmp Agent state to Enabled, set RMON state to Enabled, set Trap state to Enabled, and then click Apply. The configuration is applied on the switch.



2.6.3Switch Upgrade

Click Switch update, switch upgrading configuration tree is shown:

TFTP Upgrade:

TFTP client service - TFTP client configuration

TFTP server service - TFTP server configuration

FTP Upgrade:

FTP client service - FTP client configuration

FTP server service - FTP server configuration

2.6.3.1TFTP client configuration

Click TFTP client service. The configuration page is shown. See the equivalent CLI command at 2.5.2.2.9

The explanation of each field is as below:

Server IP address - Server IP address

Local file name - Local file name

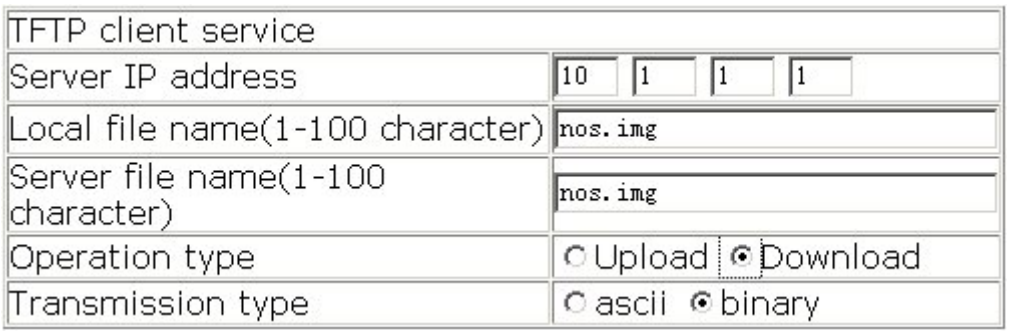
Server file name - Server file name

Operation type - Upload means to upload file, Download means to download file.

Transmission type - ascii means to transmit file in ASCII format, binary means to transmit

file in binary format

For example: Get system file nos.img from TFTP server 10.1.1.1. Input the information as below, and then click Apply



2.6.3.2TFTP server configuration

Click TFTP server service. The configuration page is shown. See the equivalent CLI command at 2.2.2.2

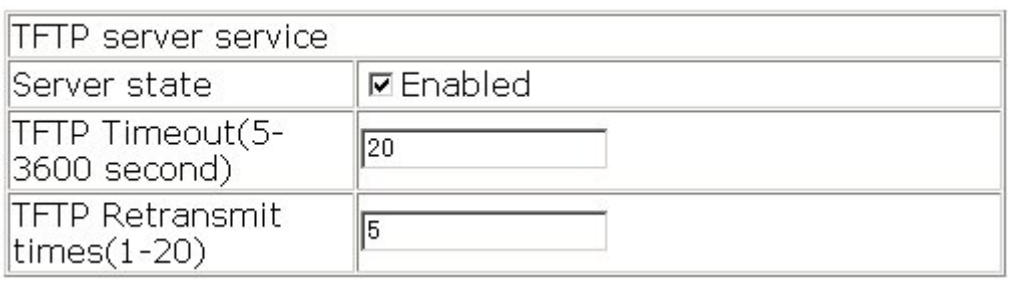
The explanation of each field is as below:

Server state - Server status, enable or disable. See the equivalent CLI command at 2.5.2.2.10

TFTP Timeout - Value of TFTP timeout. See the equivalent CLI command at 2.5.2.2.12

TFTP Retransmit times - Times of TFTP retransmit. See the equivalent CLI command at 2.5.2.2.11

For example: Enable TFTP server. Check “Enabled” box, then click Apply



2.6.3.3FTP client configuration

Click FTP client service. The configuration page is shown. See the equivalent CLI command at 2.5.2.2.3

The explanation of each field is as below:

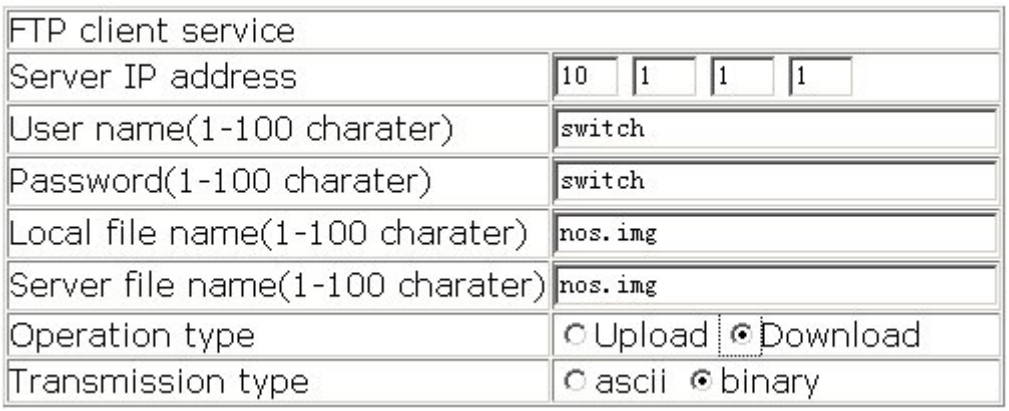
Server IP address - Server IP address

Local file name - Local file name

Server file name - Server file name

Operation type – Upload means to upload file, Download means to download file.

Transmission type—ascii means to transmit file in ASCII format, binary means to transmit file in binary format



2.6.3.4FTP server configuration

Click FTP server service. The configuration page which includes server configuration and client configuration is shown.

The explanation of each field for client configuration is as below:

FTP server state - Server state, enabled or disabled. See the equivalent CLI command at 2.5.2.2.5

FTP Timeout - FTP timeout. See the equivalent CLI command at 2.5.2.2.6

The explanation of each field for server configuration is as below:

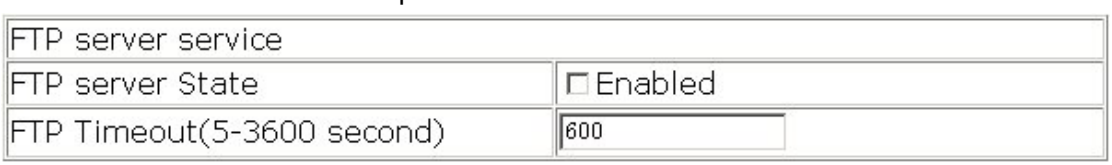
User name - User name. See the equivalent CLI command at 2.5.2.2.8

Password - Password. See the equivalent CLI command at 2.5.2.2.7

State - Status of password. Plain text means password is in plain text, Encrypted means password is encrypted. See the equivalent CLI command at 2.5.2.2.32.5.2.2.7

Remove user - Remove user. See the equivalent CLI command at 2.5.2.2.8

Add user – Add user. See the equivalent CLI command at 2.5.2.2.8



2.6.4Monitor and debug command

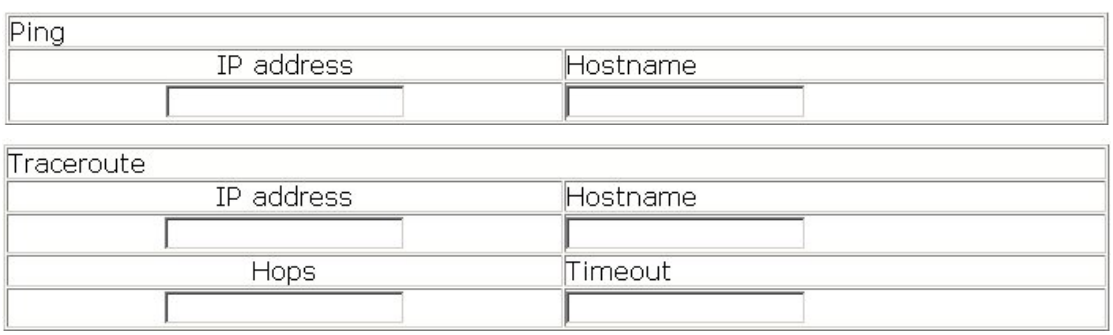
Click Basic configuration debug. The following terms are displayed.

Debug command - Debug command
Show clock - Show clock. See the equivalent CLI command at 2.2.4.1
Show flash - Show flash file information. See the equivalent CLI command at 2.2.4.3
Show history - Show recent user input history. See the equivalent CLI command at 2.2.4.4
Show running-config - Show the current effective switch configuration. See the equivalent CLI command at 2.2.4.6
Show switchport interface - Show port vlan attribute. See the equivalent CLI command at 2.2.4.8
Show tcp - Show the current TCP connection status established to the switch. See the equivalent CLI command at 2.2.4.9
Show udp - Show the current UDP connection status established to the switch. See the equivalent CLI command at 2.2.4.10
Show version - Show switch version. See the equivalent CLI command at 2.2.4.13

2.6.4.1Debug command

Click Debug command. The configuration page which includes ping and traceroute is shown. See the equivalent CLI command at 2.2.1 and at 2.2.3
The explanation of each field for Ping is as below:
IP address - Destination IP address
Hostname - Hostname

The explanation of each field for Traceroute is as below:
IP address - Target host IP address
Hostname – Hostname for the remote host
Hops - Maximum gateway number allowed
Timeout - Timeout value for test packets in milliseconds



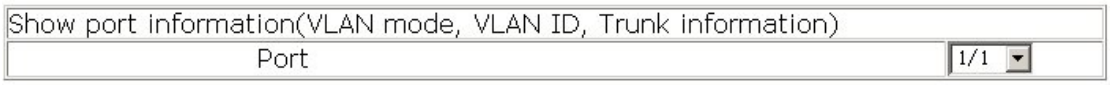
2.6.4.2Show port Vlan information

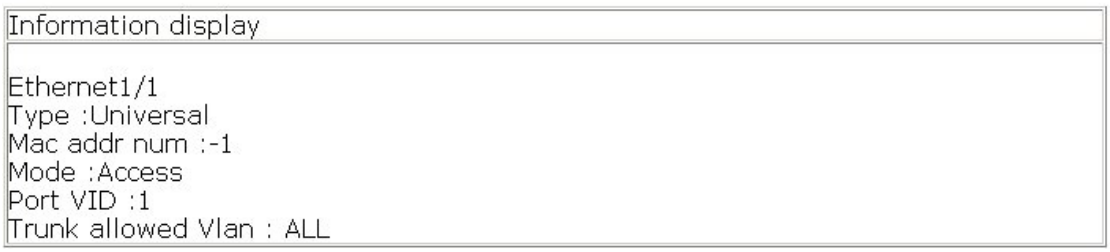
Click show switchport interface. The configuration page is shown. See the equivalent CLI command at 2.2.4.8

The explanation of each field is as below:

Port - Port list

Select port1/1, and then click Apply. The port Vlan information is shown.





2.6.4.3Other

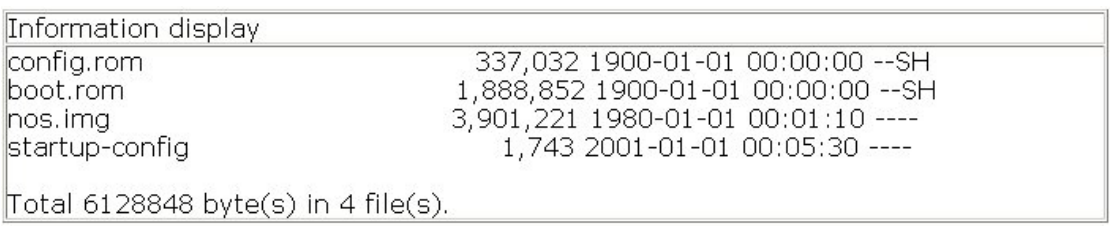
Other parts are quite straight forward. Click the node. The relevant information is shown. There is no need to input or to select.

For example:

Show clock:



Show flash file:



2.6.5Switch basic information

Click Switch basic information node, the configuration page is shown. See the equivalent CLI command at 2.2.4.13

The explanation of each field is as below:

Device type - Device type

Software version - Software version

Hardware version - Hardware version

Prompt - Command line prompt messages

Switch basic information	
Device type	ES4626
software version	1.1.0.0
Hardware version	0.0.0
prompt	ES4626

2.6.6Switch on-off configuration

Click Switch on-off information node. The configuration page is shown.

The explanation of each field is as below:

RIP Status - Enable or disable RIP. See the equivalent CLI command at 15.3.2.2.17

IGMP Snooping – Enable or disable IGMP Snooping. See the equivalent CLI command at 7.2.2.1

Switch GVRP Status – Enable or disable GVRP. See the equivalent CLI command at 5.3.2.5

Check the items, and click Apply. The configuration is applied on the switch.

Switch on-off configuration	
RIP Status	☐ Enabled
IGMP Snooping	☑ Enabled
switch GVRP Status	☐ Enabled

2.6.7Switch maintenance

On the mainpage, click Switch maintenance on the left column. Users can make the configuration of the switch maintenance.

Click Reboot to reboot the switch. See the equivalent CLI command at 2.1.10:

Reboot
Save current configuration before reboot? ◉ Yes ○ No

Click Reboot with the default configuration to delete the current configuration and reboot the switch. The default configuration is used when the switch is rebooted:

Reboot with the default configuration

2.6.8Telnet service configuration

On the mainpage, click Talent server configuration on the left column Users can configure telnet service.

Click Telnet server user configuration to configure telnet service. See the equivalent CLI command at 2.2.2.3.3:

Telnet server State – Enable or disable telnet server. See the equivalent CLI command at 2.2.2.3.3

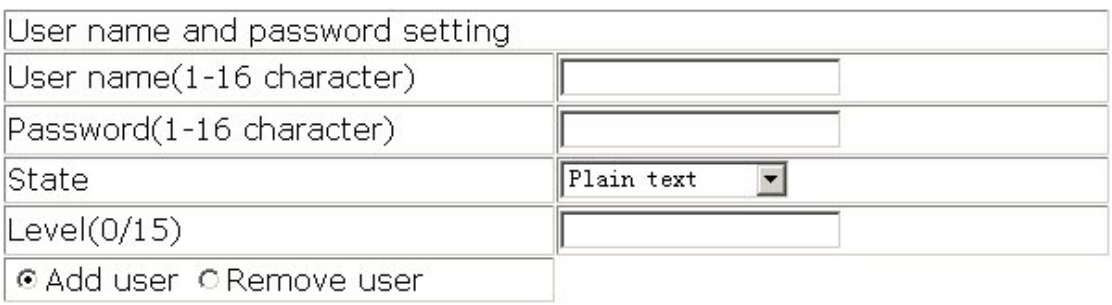


Click Telnet security IP to configure secure IP address which can configure telnet service. See the equivalent CLI command at 2.2.2.3.4:

Security IP address – Specify secure IP address

Operation – Drop-menu selection: Add Security IP address; Remove Security IP address

2.6.9username service



In username service, users can add and delete management user name and user password.

The global user can perform FTP, TFTP, Telnet and Web service.

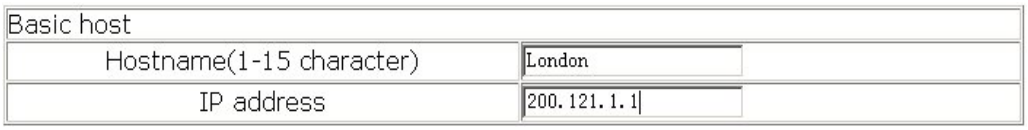
Level is the user priority. 0 refers to guest priority and 15 refers to admin priority.

State sets if the encrypted password is used.

2.6.10 Basic host configuration

- ☞ Basic host configuration - Set the mapping relationship between the host and IP address. See the equivalent CLI command at 2.1.8

Set Hostname to London, set IP address to 200.121.1.1,and then click Apply. The configuration is applied on the switch.



Chapter 3 Port Configuration

3.1 Introduction to Port

The front panel of ES4626 provide 4 Combo ports (these Combo ports can be configured as either 1000MB copper ports or 1000MB SFP fiber ports, but only one type can be selected), 20 1000MB copper ports and 2 XFP 10GB fiber port.

If the user need to configure some network ports, he/she can use the "**interface ethernet *<interface-list>***" command to enter the appropriate Ethernet port configuration mode, where ***<interface-list>*** stands for one or more ports. If ***<interface-list>*** contains multiple ports, special characters such as ";" or "-" can be used to separate ports. ";" is used for discrete port numbers and "-" is used for consecutive port number. Suppose operation should be performed to ports 2, 3, 4, 5, the command can look like this: **interface ethernet 1/2-5.** Port speed, duplex mode and traffic control can also be configured under Ethernet Port configuration Mode, and the performance of the corresponding physical network ports will change accordingly.

3.2 Port Configuration

3.2.1 Network Port Configuration

3.2.1.1 Network Port Configuration Task Sequence

1. Enter the network port configuration mode
2. Configure the properties for the network ports

Configure the combo mode for combo ports
Enable/Disable ports
Configure port names
Configure port cable types
Configure port speed and duplex mode
Configure bandwidth control
Configure traffic control
Enable/Disable port loopback function
Configure broadcast storm control function for the switch

1. Enter the Ethernet port configuration mode

Command	Explanation
Interface Mode	
interface ethernet <*interface-list*>	Enter the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Interface Mode	
combo-forced-mode { copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto } **no combo-forced-mode**	Set the combo port mode (combo ports only); the "**no combo-forced-mode**" command restores the default combo mode for combo ports, i.e. fiber ports first.
shutdown **no shutdown**	Enable/Disable specified ports
description<*string*> **no description**	Name or cancel the name of specified ports
mdi { auto | across | normal } **no mdi**	Set the cable type for the specified port; this command is not supported on the ports of 1000MB and above.
speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }	Set port speed and duplex mode of 100Base/1000Base-TX ports. The "no" format of this command restores the default setting, i.e. negotiate speed and duplex mode automatically.
negotiation **no negotiation**	Enable/Disable the auto-negotiation function of 1000Base-FX port.
rate-limit {input|output} <level> **no rate-limit {input|output}**	Set or cancel the bandwidth used for incoming/outgoing traffic for specified ports
flow control **no flow control**	Enable/Disable traffic control function for specified ports
loopback **no loopback**	Enable/Disable loopback test function for specified ports
rate-suppression {dlf | broadcast | multicast} <packets>	Enable the storm control function for broadcast, multicast and unicast for unknown destination (short for broadcast), and set allowed broadcast packet number; the "no" format of this command disables the broadcast storm control function.

3.2.1.2 Ethernet Port Configuration Commands

3.2.1.2.1 Rate-limit

Command: rate-limit {input|output} <level>

no rate-limit {input|output}

Function: Enable the bandwidth control function for the port: the "no bandwidth control**" command disables the bandwidth control function for the port.**

Parameter: <*level*>is the bandwidth limit in Mbps, the valid value ranges from 1 to 10000 M; **input** means bandwidth control applies to incoming traffic from outside the switch; **output** means bandwidth control applies to outgoing traffic to outside the switch

Command mode: Interface Mode

Default: Port bandwidth control is disabled by default.

Usage Guide: When bandwidth control is enabled for a port, and bandwidth limit is set, then the maximum bandwidth will be limited and no longer be the 10/100/1000M line speed. Note: The bandwidth limit set must not exceed the maximum physical connection speed possible of the port. For example, a bandwidth limit of 101 M (or more) cannot be set for a 10/100M Ethernet port. But for a 10/100/1000M port working less than 100 M, a bandwidth limit of 101 M (or more) is permitted.

Example: set the bandwidth limit of port 1 – 8 of slot 3 card to 40M.

Switch(Config)#interface ethernet 3/1-8

Switch(Config-Port-Range)# rate-limit input 40

Switch (Config-Port-Range)#rate-limit output 40

3.2.1.2.2 combo-forced-mode

Command: combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto }

no combo-forced-mode

Function: Set the combo port mode (combo ports only); the "**no combo-forced-mode**" command restores the default combo mode for combo ports, i.e. fiber ports first.

Parameter: copper-forced will force to use the copper cable port; **copper-preferred-auto** for copper cable port first; **sfp-forced** for fiber cable forces to use fiber cable port; **sfp-preferred-auto** for fiber cable port first.

Command mode: **Interface Mode**

Default: The default setting for combo mode of combo ports is fiber cable port first.

Usage Guide: The combo mode of combo ports and the port connection condition determines the active port of the combo ports. A combo port consists of one fiber port and a copper cable port. It should be noted that the speed-duplex command applies to the copper cable port while the negotiation command applies to the fiber cable port, so they will not conflict. Only one of the fiber cable port or the copper cable port of the same combo port can be active at a time. Only the active port can send and receive data normally.

For the determination of active port in a combo port, see the table below. The headline row in the table indicates the combo mode of the combo port, while the first column indicates the connection conditions of the combo port, in which “connected” refers to a good connection of fiber cable port or copper cable port to the other devices.

	Copper forced	**Copper preferred**	**SFP forced**	**SFP preferred**
Fiber connected, copper not connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port
Copper connected, fiber not connected	Copper cable port	Copper cable port	Fiber cable port	Copper cable port
Both fiber and copper are connected	Copper cable port	Copper cable port	Fiber cable port	Fiber cable port
None of fiber and copper are connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port

Note:

- ☞ Combo port is a conception involving physical layer and the LLC sublayer of datalink layer. The status of combo port will not affect any operation in the MAC sublayer of datalink layer and upper layers. If the bandwidth limit for a combo port is 1 Mb, then this 1 Mb applies to the active port of this combo port, regardless of the port type being copper or fiber.
- ☞ If a combo port connects to another combo port, it is recommended for both parties to use copper- or fiber-forced mode.
- ☞ Run “show interfaces status” under Admin Mode to check for the active port of a combo port The following result indicates the active port for a combo port is the fiber cable port (or copper cable port): Hardware is Gigabit-combo, active is fiber (copper).

Example: Set Port 1/25 -28 to fiber-forced.

Switch(Config)#interface ethernet 1/25-28

Switch(Config-Port-Range)#combo-forced-mode sfp-forced

3.2.1.2.3 flow control

Command: flow control

no flow control

Function: Enable the flow control function for the port: the "**no flow control"** command disables the flow control function for the port**.**

Command mode: Interface Mode

Default: Port flow control is disabled by default.

Usage Guide: After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. The ports of ES4626/ES4650 support 802.3X fallback flow control ; the ports work in half duplex mode, supporting fallback flow control. If the fallback control may result in serious HOL, the switch will automatically start HOL control (discard some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Note: Port flow control function is NOT recommended unless the user needs a slow speed, low performance network with low packet loss. Flow control will not work between different cards in the switch. When enable the port flow control function, speed and duplex mode of both ends should be the same.

Example: Enable the flow control function in ports 1/1-8.

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#flow control

3.2.1.2.4 interface ethernet

Command: interface ethernet <*interface-list*>

Function: Enter Ethernet Interface Mode from Global Mode.

Parameter: <*interface-list*> stands for port number.

Command mode: Global Mode

Usage Guide: Run *exit* command will exit the Ethernet Interface Mode to Global Mode.

Example: Enter the Ethernet Interface Mode for port 1/1, 2/4-5, 3/8.

Switch(Config)#interface ethernet 1/1;2/4-5;3/8

Switch(Config-Port-Range)#

3.2.1.2.5 loopback

Command: loopback

no loopback

Function: Enable the loopback test function in Ethernet port; the "**no loopback**" command disables the loopback test on Ethernet port.

Command mode: Interface Mode

Default: Loopback test is disabled in Ethernet port by default.

Usage Guide: Loopback test can be used to verify the Ethernet ports are working normally. After loopback enabled, the port will assume a connection established to itself, and all traffic send from the port will receive in this very port.

Default: Enable loopback test in Ethernet ports 1/1 – 8.

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#loopback

3.2.1.2.6 mdi

Command: mdi { auto | across | normal }

no mdi

Function: Sets the cable types supported by the Ethernet port; the "**no mdi**" command sets cable type auto-identification. This command is not supported on the ES4626/ES4650 ports of 1000MB and above, these ports have auto-identification set for cable types.

Parameter: auto indicates auto identification of cable types; **across** indicates crossover cable support only; **normal** indicates straight-through cable support only.

Command mode: Interface Mode

Default: Port cable type is set to auto-identification by default.

Usage Guide: Auto-identification is recommended. Generally, straight-through cable is used for switch-PC connection and crossover cable is used for switch-switch connection.

Example: Set the cable type support of Ethernet ports 3/5 – 8 to straight-through cable only.

Switch(Config)#interface ethernet 3/5-8

Switch(Config-Port-Range)#mdi normal

3.2.1.2.7 description

Command: description <*string*>

no description

Function: Sets a name for the specified port "**no name**" command cancels the setting.

Parameter: <*string*> is a string, up to 32 characters are allowed.

Command mode: Interface Mode

Default: No name is set by default.

Usage Guide: This command facilitates the management of the switch. The user can name the ports according to their usage, for example, 1/1-2 ports used by the financial department, and they can be named "financial"; 2/9 port is used by the engineering department, and can be named "engineering"; 3/12 port connects to the server, and can be named "Servers". Thus the usage of the ports are obvious.

Example: Name ports 1/1-2 as "financial".

Switch(Config)#interface ethernet 1/1-2

Switch(Config-Port-Range)# descriptionfinancial

3.2.1.2.8 negotiation

Command: negotiation no negotiation

Function: Enable the auto-negotiation function of 1000Base-FX port. Use the "no" command to disable the auto-negotiation function of 1000Base-FX port. **Command mode:** Port configuration Mode

Default: Auto-negotiation is enabled by default.

Usage Guide: This command applies to 1000Base-FX interface only. The **negotiation** command is not available for 1000Base-TX or 100Base-TX interface. . For combo port, this command applies to the 1000Base-FX port only and has no effect on 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use **speed-duplex** command instead.

Example: Port 1 of Switch1 is connected to port 1 of Switch2, the following will disable the negotiation for both ports.

Switch1(Config)#interface e1/1

Switch1(Config-Ethernet1/1)# no negotiationSwitch2(Config)#interface e1/1

Switch2(Config-Ethernet1/1)#negotiation

3.2.1.2.9 rate-suppression

Command: rate-suppression {dlf | broadcast | multicast} <packets>

no rate-suppression {dlf | broadcast | multicast}

Function: Sets the traffic limit for broadcast, multicast and unicast for unknown destination on all ports in the switch; the "**no rate-suppression**" command disables the traffic throttle function of broadcast, multicast and unicast for unknown destination on all ports in the switch, i.e., enable broadcast, multicast and unicast for unknown destination

to pass through the switch at line speed.

Parameter: use **dlf** to limit unicast traffic for unknown destination; **multicast** to limit multicast traffic; **broadcast** to limit broadcast traffic. ***<packets>*** **s**tands for the number of packets allowed to pass through per second for non-10Gb ports; for 10 Gb ports, this is the number of packets allowed to pass through multiplies 1,040. The valid range for both ports is 1 to 262,143.

Command mode: Interface Mode

Default: no limit is set by default, broadcast, multicast and unicast for unknown destination are allowed to pass at line speed.

Usage Guide: All the ports in the switch belong to a same broadcast domain if no VLAN is set. The switch will send the abovementioned three traffics to all the ports in the broadcast domain, which may result in broadcast storm. Broadcast storm can greatly degrade the switch performance, enabling broadcast storm control function can protect the switch from broadcast storm to the best possibility. Note the difference of this command in 10 Gb ports and other ports. If the allowed traffic is set to 3, it means to allow 3120 packets per second and discard the rest for 10 Gb ports; while the same setting for non-10 Gb ports means to allow 3 broadcast packets per second and discard the rest.

Example: Set port 8 – 10(1000Mb) of slot 2 to allow 3 broadcast packets per second.

Switch(Config)#interface ethernet 2/8-10

Switch(Config-Port-Range)#rate-suppression broadcast 3

3.2.1.2.10 shutdown

Command: shutdown

no shutdown

Function: Shut down the specified Ethernet port; the "**no shutdown**" command enables the port.

Command mode: Interface Mode

Default: Ethernet port is enable by default.

Usage Guide: When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user typed "**show interfaces status**" command is "down".

Example: Enable ports 1/1-8.

Switch(Config)#interface ethernet1/1-8

Switch(Config-Port-Range)#no shutdown

3.2.1.2.11 speed-duplex

Command: speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }

no speed-duplex

Function: Set the speed and duplex mode for 1000Base-TX or 100Base-TX ports; the "**no speed-duplex**" command restores the default speed and duplex mode setting, i.e. auto speed negotiation and duplex.

Parameter: auto for auto speed negotiation; **force10-half** for forced 10Mb/s at half duplex; **force10-full** for forced 10Mb/s at full duplex mode; **force100-half** for forced 100Mb/s at half duplex mode; **force100-full** for forced 100Mb/s at full duplex mode; **force1g-half** for forced 1000Mb/s at half duplex mode; **force1g-full** for forced 1000Mb/s at full duplex mode; **nonegotiate** for disable auto negotiation for 1000 Mb port; **master** for force the 1000 Mb port to be **master** mode; **slave** for force the 1000 Mb port to be **slave** mode.

Command mode: Port configuration Mode.

Default: Auto negotiation for speed and duplex mode is set by default.

Usage Guide: This command applies to 1000Base-TX or 100Base-TX ports only.

speed-duplex command is not available for 1000Base-FX port. For combo port, this command applies to the 1000Base-TX port only and has no effect on 1000Base-FX port. To change the negotiation mode of 1000Base-FX port, use **negotiation** command instead.

When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e. if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

1000Gb ports are defaulted to **master** when configuring **nonegotiate** mode. If one end is set to **master** mode, the other end must be set to **slave** mode.

force1g-half Is not supported yet.

Example: Port 1 of Switch1 is connected to port 1 of Switch2, the following will set both ports in forced 100Mb/s at half duplex mode.

```
Switch1(Config)#interface e1/1
Switch1(Config-Ethernet1/1)#speed-duplex force100-half
Switch2(Config)#interface e1/1
Switch2(Config-Ethernet1/1)#speed-duplex force100-half
```

3.2.2 VLAN Interface Configuration

3.2.2.1 VLAN Interface Configuration Task Sequence

1. Enter VLAN Mode
2. Configure the IP address for VLAN interface and enables VLAN interface.

1. Enter VLAN Mode

Command	Explanation
Global Mode	
ip address {<*ip-address*> <*mask*> [secondary] | bootp | dhcp} **no ip address [<*ip-address*> <*mask*>]**	Enter VLAN Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes specified VLAN interface or startup client protocol for bootp/dhcp

2. Configure the IP address for VLAN interface and enables VLAN interface.

Command	Explanation
VLAN Mode	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configure the VLAN interface IP address; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes VLAN interface IP address.
VLAN Mode	
shutdown **no shutdown**	Enable/Disable VLAN interface

3.2.2.2 VLAN Interface Configuration Commands

3.2.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Enter VLAN Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes existing VLAN interface. .

Parameter: <*vlan-id*> is the VLAN ID for the establish VLAN, valid range is 1 to 4094.

Command mode: Global Mode

Usage Guide: Before setting a VLAN interface, the existence of the VLAN must be verified. Run the *exit* command will exit the VLAN Mode to Global Mode.

Example: Enter the VLAN Interface Mode for VLAN1.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#

3.2.2.2.2 ip address

Command: ip address{<*ip-address*> <*mask*> [secondary] | bootp | dhcp} no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Set the IP address and mask for the switch; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the specified IP address setting.

Parameter: <*ip-address*> is the IP address in dot decimal format; **<*mask*>** is the subnet mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Command mode: VLAN Interface Mode

Default: No IP address is configured by default.

Usage Guide: This command configures IP address for VLAN interface manually. If the optional parameter secondary is not present, the IP address will be the primary IP of the VLAN interface, otherwise, the IP address configured will be the secondary IP address for the VLAN interface. A VLAN interface can have only one primary IP address but multiple secondary IP address. Both primary IP address and secondary IP address can be used for SNMP/Web/Telnet management. In addition, ES4626/ES4650allows IP address to be obtained through BootP/DHCP.

Example: Set the IP address of VLAN1 interface to 192.168.1.10/24.

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

3.2.2.2.3 shutdown

Command: shutdown

no shutdown

Function: Shut down the specified VLAN Interface; the "**no shutdown**" command enables the VLAN interface.

Command mode: VLAN Interface Mode

Default: VLAN Interface is enable by default.

Usage Guide: When VLAN interface is shutdown, no data frames will be sent by the VLAN interface. If the VLAN interface need to obtain IP address via BootP/DHCP protocol, it must be enabled.

Example: Enable VLAN1 interface of the switch.

Switch(Config-If-Vlan1)#no shutdown

3.2.3 Port Mirroring Configuration

3.2.3.1 Introduction to Port Mirroring

Port mirroring refers to duplicate the data frames sent/received on a port to another port, where the duplicated port is referred to as mirror source port, and the duplicating port is referred to as mirror destination port. A protocol analyzer (such as Sniffer) or RMON monitoring instrument is often attached to the mirror destination port to monitor and manage the network and diagnostic.

ES4626/ES4650 support one mirror destination port only. The number of mirror source port is not limited, one or more ports can be used. Multiple source ports can be within the same VLAN or across several VLANs. The destination port and source port(s) can locate in different VLANs.

3.2.3.2 Port Mirroring Configuration Task Sequence

1. Specify mirror source port
2. Specify mirror destination port

1. Specify mirror source port

Command	Explanation
Port configuration mode	
port monitor <*interface-list*> [rx| tx| both] no port monitor <*interface-list*> no port monitor <*interface-list*>	Specify mirror source port; the " **no monitor session <*session*> {interface <*interface-list*> | cpu [slot <*slotnum*>]}**" command deletes mirror port.

3.2.3.3 Port Mirroring Configuration

3.2.3.3.1 port monitor

Command: port monitor <*interface-list*> [rx| tx| both]

no port monitor <*interface-list*>

Parameter: <*interface-list*> is the list of the monitored source interfaces; **rx** is the inbound traffic of the monitored source interface; **tx** is the outbound traffic of the monitored source interface; **both** is the inbound and outbound traffic of the monitored source interface.

Command mode: Interface Mode

Default: There is no monitored interface by default. After this function is enabled, the inbound and outbound traffic on the source interface is monitored by default.

Usage Guide: The source interface and the destination interface must have the same speed; otherwise some packets will be lost. Multiple source interfaces can be monitored on a single destination interface.

Example: On the interface 1/11, monitor the inbound and outbound traffic of the source interface 1/6.

Switch(config)#interface Ethernet 1/11

Switch(Config-Ethernet1/11)#port monitor Ethernet 1/6 both

3.2.3.4 Port Mirroring Examples

See “Port Configuration Examples”.

3.2.3.5 Device Mirroring Troubleshooting Help

3.2.3.5.1 Monitor and Debug Commands

3.2.3.5.1.1 show port monitor

Command: show port monitor [interface <*interface-list*>]

Function: Display information about mirror source/destination ports.

Parameter: <*interface-list*>*is*** the mirror source port(s)

Command mode: Admin Mode

Usage Guide: This command displays the mirror source port(s) and destination port currently configured.

Example:

Switch#show port monitor

3.2.3.5.2 Device Mirroring Troubleshooting Help

If problems occur configuring port mirroring, please check the following first for causes:

- ☞ Whether the mirror destination port is a member of a trunk group or not, if yes, modify the trunk group.
- ☞ If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports or duplicate traffic of one direction only, or choose a port with greater throughput as the destination port.

3.3 Port Configuration Example

No VLAN has been configure in the switches, the default VLAN1 is used.

Switch	Port	Property
SW1	2/7	Ingress bandwidth limit: 150 M
SW2	1/8	Mirror source port
	3/9	100M/full, mirror source port
	4/12	1000M/full, mirror destination port
SW3	4/10	100M/full

The configurations are listed below:

SW1:

Switch1(Config)#interface ethernet 1/7

Switch1(Config-Ethernet1/7)# rate-limit input 150

Switch1(Config-Ethernet1/7)#rate-limit output 150

SW2:

Switch2(Config)#interface ethernet 1/9

Switch2(Config-Ethernet1/9)# speed-duplex force100-full

Switch2(Config-Ethernet1/9)#exit

Switch2(Config)#interface ethernet 1/12

Switch2(Config-Ethernet1/12)# speed-duplex force1000-full

Switch2(Config-Ethernet1/12)#port monitor interface ethernet1/8;1/9 both

Switch2(Config-Ethernet1/12)#exit

SW3:

Switch3(Config)#interface ethernet 1/10

Switch3(Config-Ethernet1/10)# speed-duplex force100-full

Switch3(Config-Ethernet1/10)#duplex full

3.4 Port Troubleshooting Help

3.4.1 Monitor and Debug Commands

3.4.1.1 clear counters

Command: clear counters [{ethernet <*interface-list*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]

Function: Clear the statistics of the specified port.

Parameter: <*interface-list*> stands for the Ethernet port number; **< *vlan-id* >** stands for the VLAN interface number; **<*port-channel-number*>** for trunk interface number; **<*interface-name*>** for interface name, such as port-channel1.

Command mode: Admin Mode

Default: Port statistics are not cleared by default.

Usage Guide: If no port is specified, then statistics of all ports will be cleared.

Example: Clear the statistics for Ethernet port 1/1.

Switch#clear counters ethernet 1/1

3.4.1.2 show interfaces status

Command: show interfaces status **[{ethernet <*interface-number*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]**

Function: Display information about specified port.

Parameter: <*interface-number*> stands for the Ethernet port number; **< *vlan-id* >** stands for the VLAN interface number; **<*port-channel-number*>** for trunk interface number; **<*interface-name*>** for interface name, such as port-channel1.

Command mode: Admin Mode

Default: No port information is displayed by default.

Usage Guide: for Ethernet port, this command displays information about port speed, duplex mode, traffic control on/off, broadcast storm control and statistics for packets sent/received; for VLAN interface, this command displays MAC address, IP address and statistics for packets sent/received; for trunk port, this command displays port speed,

duplex mode, traffic control on/off, broadcast storm control and statistics for packets sent/received. Usage Guide: If no port is specified, then information for all ports will be displayed.

Example: Display information about port 4/1.

Switch#show interfaces status ethernet 4/1

3.4.2 Port Troubleshooting Help

Here are some situation frequently occurs in port configuration and the advised solutions:

- ☞ Two connected fiber interfaces won't link up if one interface is set to auto negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- ☞ The following combinations are not recommended: enable traffic control as well as set multicast limit for the same port; set broadcast, multicast and unicast for unknown destination control as well as port bandwidth limit for the same port. If such combinations are set, the port throughput may fall below the expected performance.

3.5 WEB Management

Click Port configuration, the port configuration page is shown. Users can configure switch ports features such as port speed and port duplex etc.

3.5.1Ethernet port configuration

Click Port configuration, Ethernet port configuration. The Ethernet port configuration page is shown. Users can configure Ethernet ports features, such as port speed, port duplex and bandwidth control etc.

3.5.1.1Physical port configuration

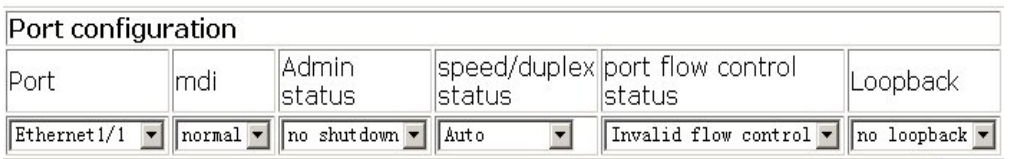
Click Port configuration, Ethernet port configuration, Physical port configuration. The following port features can be configured:

- ☞ Port - Specify the port
- ☞ mdi – Set the supported cable types on the Ethernet port. Auto means automatic detected; across means that only the crossover

cable is support; normal means that only the straight cable is support. See the equivalent CLI command at 3.2.1.2.6

- ☞ Admin Status – Enable or disable port. See the equivalent CLI command at 3.2.1.2.9
- ☞ speed/duplex status – Set port duplex. The supported types include: auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half and 1000M/Full. See the equivalent CLI command at 3.2.1.2.2 and 3.2.1.2.10
- ☞ port flow control status – Configure port flow control. See the equivalent CLI command at 3.2.1.2.3
- ☞ Loopback – Set to allow or not to allow loopback test. See the equivalent CLI command at 3.2.1.2.5

For example: Specify port as Ethernet1/1; set mdi to normal; set Admin Status to no shutdown; set speed/duplex status to auto; set port flow control status to Invalid flow control; set Loopback to no loopback, and then click Apply. The configuration is applied on the port 1/1.



The switch port information is shown in post list page:

Port list

Port	mdi	Status	Speed	Mode	Flow control	loopback
Ethernet1/1	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/2	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/3	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/4	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/5	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/6	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/7	auto	UP	auto	auto	Non flow control state	no loopback
Ethernet1/8	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/9	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/10	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/11	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/12	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/13	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/14	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/15	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/16	auto	DOWN	auto	auto	Non flow control state	no loopback

3.5.1.2 Bandwidth control

Click Port configuration, Ethernet port configuration, Bandwidth control. Users can configure port bandwidth control. See the equivalent CLI command at 3.2.1.2.1

- Port – Specify the port
- Bandwidth control level – Port bandwidth control; valid ranges is 1 to 10000 in Mbps.
- Control type –input and output means that bandwidth control is applied to the inbound and outbound traffic; input means that bandwidth control is only applied to the inbound traffic; output means that bandwidth control is only applied to the outbound traffic.

For example: Specify port as Ethernet1/1; set Bandwidth control level to 5000; set Control type to input, and then click Apply. The configuration is applied on the port 1/1.



The switch port information is shown in post list page:

Port list

Port Num	Ingress bandwidth threshold(Mb)	Outgress bandwidth threshold(Mb)
Ethernet1/1	100000	100000
Ethernet1/2	100000	100000
Ethernet1/3	100000	100000
Ethernet1/4	100000	100000
Ethernet1/5	100000	100000
Ethernet1/6	100000	100000
Ethernet1/7	100000	100000
Ethernet1/8	100000	100000
Ethernet1/9	100000	100000
Ethernet1/10	100000	100000
Ethernet1/11	100000	100000
Ethernet1/12	100000	100000
Ethernet1/13	100000	100000
Ethernet1/14	100000	100000
Ethernet1/15	100000	100000

3.5.2 Vlan interface configuration

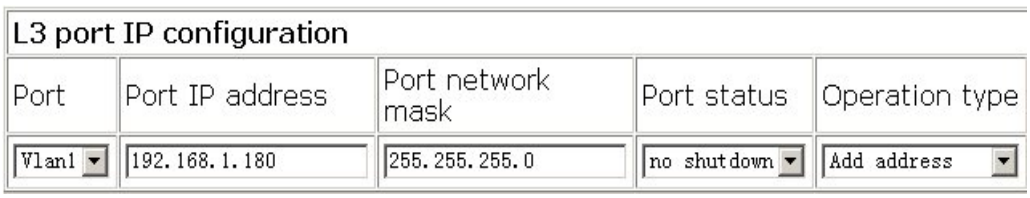
Click Port configuration, Vlan interface configuration. The VLAN port configuration page is shown. Users can configure port Layer 3 information such as IP address and network mask etc.

3.5.2.1 Allocate IP address for L3 port

Click Port configuration, Vlan interface configuration, Allocate IP address for L3 port. Users can configure port Layer 3 IP address. See the equivalent CLI command at 3.2.2.2.2:

- Port – Specify port
- Port IP address – Port Layer 3 IP address
- Port network mask – Port network mask
- Port status – Port Layer 3 status
- Operation type – Add or delete IP address

For example: Specify port as Vlan1; set Port IP address to 192.168.1.180; set Port network mask to 255.255.255.0; set Port status to no shutdown; set Operation type to Add address, and then click Apply. The configuration is applied on the switch.

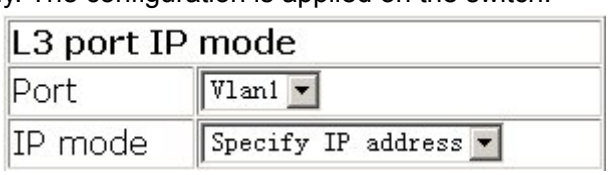


3.5.2.2 L3 port IP addr mode configuration

Click Port configuration, Vlan interface configuration, L3 port IP addr mode configuration. Users can configure the mode of obtaining IP address of the port:

- Port – Specify the port
- IP mode – Specify IP address means users specify the IP address manually; bootp-client means IP address is obtained by BootP. See the equivalent CLI command at 3.3.2.2; dhcp-client means that IP address is obtained by DHCP. See the equivalent CLI command at 3.3.2.2.

For example: Specify port as Vlan1; set IP mode to Specify IP address, and then click Apply. The configuration is applied on the switch.



3.5.3 Port mirroring configuration

Click Port configuration, Port mirroring configuration. Users can configure port mirroring.

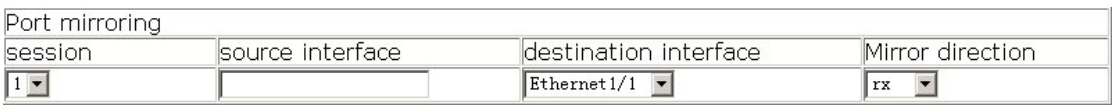
3.5.3.1 Mirror configuration

Click Port configuration, Port mirroring configuration, Mirror configuration. Users can configure port mirroring for source interface and destination interface.

Source Interface configuration. See the equivalent CLI command at 3.2.3.3.1:

- session – Mirroring session
- source interface list – Source interface list for mirroring
- Mirror direction – rx means that received traffic is mirrored; tx means sent traffic is mirrored; both means both received and sent traffic is mirrored.

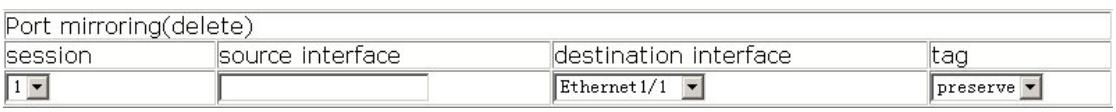
For example: Select session 1; set source interface to eth1/1-4, set Mirror direction to rx, and then click Apply. The configuration is applied on the switch.



Destination Interface configuration. See the equivalent CLI command at 3.2.3.3.2:

- session – Mirroring session
- destination interface – destination interface for mirroring
- tag – Set the vlan tag of the packets sent by the destination interface. All means that all the packets have vlan tag; preserve mean that if the packets with vlan tag when they enter the switch, they keep vlan tag when they are sent out. If the packets without vlan tag when they enter the switch, they don't have vlan tag when they are sent out.

For example: Select session 1; set source interface to 1/5; set tag to preserve, and then click Apply. The configuration is applied on the switch.



3.5.4 Port debug and maintenance

Click Port configuration, Port debug and maintenance. It is used to enable port debug management list for obtaining port information.

3.5.4.1Show port information

Click Port configuration, Port debug and maintenance, Show port information. The port statistics information is shown. See the equivalent CLI command at 3.4.1.2

For example: Select to display Ethernet1/1, and then click Refresh. The statistics information of port Ethernet 1/1 is shown.



Port statistics	
Single Collision Frames	0
Multiple Collision Frames	0
SQE Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
Mac Transmit Errors	0
Carrier Sense Errors	0
Mac Receive Errors	0
Ether Chip Set	0
Broadcast Pkts	0
Fragments	0
Jabbers	0

Item	Receiving statistics	Transmitting statistics
Datagram	0	2
Octets	0	136
Errors	0	0
Discarded	0	0
Ip datagram	0	0

Packet size	Received
less than 64	0
64	0
65--127	2
128--255	0
256--511	0
512--1023	0
1024--1518	0

Refresh

Chapter 4 MAC Table Configuration

4.1 Introduction to MAC Table

MAC table is a table identifies the mapping relationship between destination MAC addresses and switch ports. MAC addresses can be categorized as static MAC addresses and dynamic MAC addresses. Static MAC addresses are manually configured by the user, have the highest priority and are permanently effective (will not be overwritten by dynamic MAC addresses); dynamic MAC addresses are entries learnt by the switch in data frame forwarding, and is effective for a limited period. When the switch receives a data frame to be forwarded, it stores the source MAC address of the data frame and creates a mapping to the destination port. Then the MAC table is queried for the destination MAC address, if hit, the data frame is forwarded in the associated port, otherwise, the switch forwards the data frame to its broadcast domain. If a dynamic MAC address is not learnt from the data frames to be forwarded for a long time, the entry will be deleted from the switch MAC table.

There are two MAC table operations:

1. Obtain a MAC address;
2. Forward or filter data frame according to the MAC table.

4.1.1 Obtaining MAC Table

The MAC table can be built up by static configuration and dynamic learning. Static configuration is to set up a mapping between the MAC addresses and the ports; dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

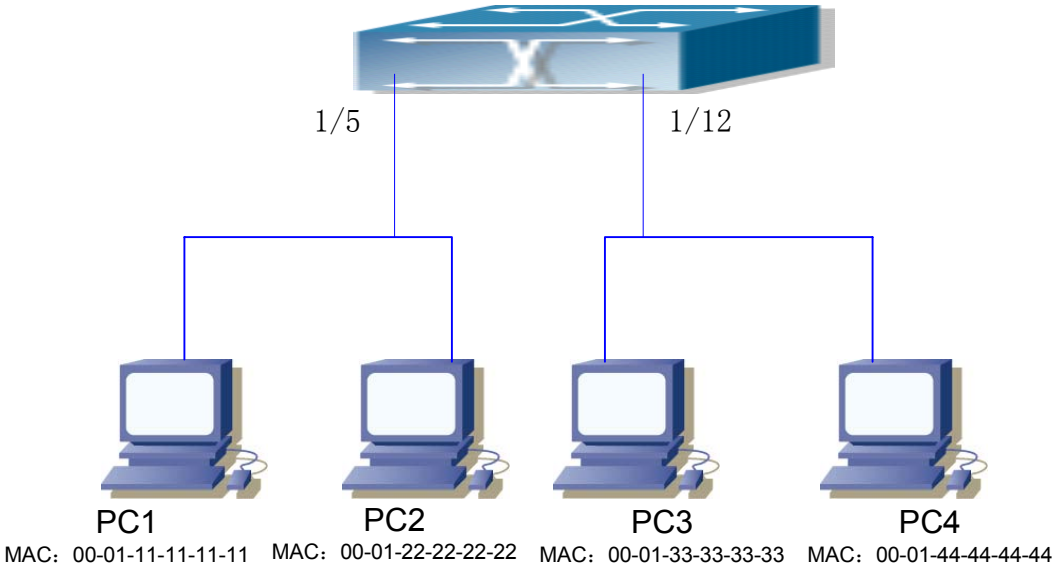


Fig 4-1 MAC Table dynamic learning

The topology of the figure above: 4 PCs connected to ES4626/ES4650, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 1/5 of ES4626/ES4650; PC3 and PC4 belongs to the same physical segment that connects to port 1/12 of ES4626/ES4650.

The initial MAC table contains no address mapping entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process likes the following:

1. When PC1 is sending a message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 for this message, the mapping entry of 00-01-11-11-11-11 and port 1/5 is added to the switch MAC table.
2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port 1/5, and no port mapping for 00-01-33-33-33-33 present, the switch broadcast this message to all the ports in the switch (assuming all ports belong to the default VLAN0.
3. PC3 and PC4 on port 1/12 receive the message sent by PC1, but PC4 will not reply, as the destination MAC address is 00-01-33-33-33-33, only PC3 will reply to PC1. When port 1/12 receives the message sent by PC3, a mapping entry for MAC address 00-01-33-33-33-33 and port 1/12 is added to the MAC table.
4. Now the MAC table has two dynamic entries, MAC address 00-01-11-11-11-11 - port 1/5 and 00-01-33-33-33-33 – port 1/12.
5. After the communication between PC1 and PC3, the switch does not receive any message sent from PC1 and PC3. And the MAC address mapping entries in the MAC table are deleted after 300 seconds. The 300 seconds here is the default aging time

for MAC address entry in ES4626/ES4650. Aging time can be modified in ES4626/ES4650.

4.1.2 Forward or Filter

The switch will forward or filter received data frames according to the MAC table. Take the above figure as an example, assuming ES4626/ES4650 has learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of ES4626/ES4650 will be:

MAC Address	Port number	Entry added by
00-01-11-11-11-11	1/5	Dynamic learning
00-01-22-22-22-22	1/5	Static configuration
00-01-33-33-33-33	1/12	Dynamic learning
00-01-44-44-44-44	1/12	Static configuration

1. Forward data according to the MAC table

If PC1 sends a message to PC3, the switch will forward the data received on port 1/5 from port 1/12.

2. Filter data according to the MAC table

If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e. drop this message).

Three types of frames can be forwarded by the switch:

- ✧ Broadcast frame
- ✧ Multicast frame
- ✧ Unicast frame

The following describes how the switch deals with all the three types of frames:

1. Broadcast frame: The switch can segregate collision domains but not broadcast domains. If no VLAN is set, all devices connected to the switch are in the same broadcast domain. When the switch receives a broadcast frame, it forwards the frame in all ports. When VLANs are configured in the switch, the MAC table will be adapted accordingly to add VLAN information. In this case, the switch will not forward the received broadcast frames in all ports, but forward the frames in all ports in the same VLAN.
2. Multicast frame: When IGMP Snooping function is not enabled, multicast frames are processed in the same way as broadcast frames; when IGMP Snooping is enabled, the switch will only forward the multicast frame to the ports belonging to the very multicast group.
3. Unicast frame: When no VLAN is configured, if the destination MAC addresses are in the switch MAC table, the switch will directly forward the frames to the associated

ports; when the destination MAC address in a unicast frame is not found in the MAC table, the switch will broadcast the unicast frame. When VLANs are configured, the switch will forward unicast frame within the same VLAN. If the destination MAC address is found in the MAC table but belonging to different VLANs, the switch can only broadcast the unicast frame in the VLAN it belongs to.

4.2 MAC Table Configuration

4.2.1 mac-address-table aging-time

Command: mac-address-table static <*mac-addr*> interface <*interface-name*>

vlan <*vlan-id* > no mac-address-table [<*mac-addr*>] [interface <*interface-name*>] [vlan <*vlan-id*>] [static| dynamic]

Function: Set the aging time for address mapping entries in the MAC table dynamically learnt; the "**no mac-address-table aging-time**" command restores the aging time to the default 300 seconds.

Parameter: < *age*> is the aging time in seconds, the valid range is 10 to 100000; 0 for no aging.

Command mode: Global Mode

Default: The system default aging time is 300 seconds.

Usage Guide: Too short aging time results in many unnecessary broadcasts and causing performance degradation; too long aging time will leave some obsolete entries occupying the space of MAC table. For this reason, the user should set a reasonable aging time according to the production conditions.

If the aging time is set to 0, addresses dynamically learned by the switch will not age in time, the addresses learned will be kept in the MAC table permanently.

Example: Set the aging time for dynamically learned entries in the MAC table to 400 seconds.

Switch(Config)#mac-address-table aging-time 400

4.2.2 mac-address-table static

Command: mac-address-table static address <*mac-addr*> vlan <*vlan-id*> interface <*interface-name*>

no mac-address-table [{static | dynamic} [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]]

Function: Add or modify static address entry , the "**no mac-address-table**" command delete static address entries and dynamic address entries.

Parameter: static stands for static address entry; **dynamic** for dynamic address entry; ***<mac-addr>*** for MAC address to add or delete; ***<interface-name>*** for port name to forward the MAC frame; ***<vlan-id>*** for VLAN number.

Command mode: Global Mode

Default: When configuring VLAN interface, the system will generate a static address mapping entry for a system inherent MAC address and the VLAN number.

Usage Guide: For some special purpose or if the switch can not learn MAC address dynamically, the user can use this command to establish mapping relationship between MAC addresses and ports/VLAN.

"**no mac-address-table**" command will delete all existing dynamic, static and filter MAC address entries, except system default reserved entries.

Example: Port 1/1 belongs to VLAN200, set a mapping to MAC address 00-03-0f-f0-00-18.

Switch(Config)#mac-address-table static 00-03-0f-f0-00-18 interface Ethernet 1/5 vlan 200

4.2.3 mac-address-table discard

Command: mac-address-table static <*mac-addr*> discard vlan <*vlan-id* >

no mac-address-table [<*mac-addr*>] discard [vlan <*vlan-id*>]

Function: Add or modify filter address entry , the "**no mac-address-table blackhole**" command delete filter address entries.

Parameter: blackhole stands for a filter entry, filter entries is configured to discard frames of specified MAC addresses, so that traffic can be filtered. Both source addresses and destination addresses can be filtered. ***<mac-addr>*** stands for MAC addresses to be added or deleted, ***<vlan-id>*** for VLAN number.

Command mode: Global Mode

Usage Guide: "**no mac-address-table blackhole**" command will delete all filter MAC address entries in the switch MAC table.

Example: Set 00-03-0f-f0-00-18 to be a filter MAC address entry for VLAN200.

Switch(Config)# mac-address-table static 00-03-0f-f0-00-18 discard vlan 200

4.3 Typical Configuration Examples

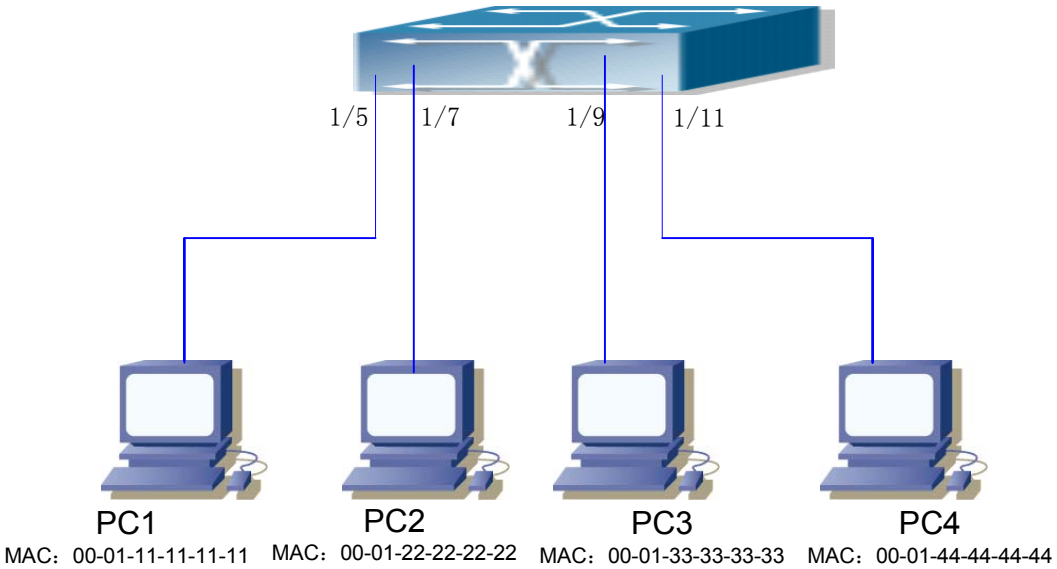


Fig 4-2 MAC Table typical configuration example

Scenario: Four PCs as shown in the above figure connect to port 1/5, 1/7, 1/9, 1/11 of switch, all the four PCs belong to the default VLAN1. As required by the network environment, dynamic learning is enabled. PC1 holds sensitive data and can not be accessed by any other PC that is in another physical segment; PC2 and PC3 have static mapping set to port 7 and port 9, respectively.

The configuration steps are listed below:

1. Set the MAC address 00-01-11-11-11-11 of PC1 as a filter address.

Switch(Config)# mac-address-table static 00-01-11-11-11-11 discard vlan 12. Set the static mapping relationship for PC2 and PC3 to port 7 and port 9, respectively.

Switch(Config)# mac-address-table static 00-01-22-22-22-22 interface ethernet 1/7 vlan 1

Switch(Config)#mac-address-table static 00-01-33-33-33-33 interface ethernet 1/9 vlan 1

4.4 Troubleshooting Help

4.4.1 Monitor and Debug Commands

4.4.1.1 show mac-address-table

Command: show mac-address-table [static|aging-time|discard] [address <*mac-addr*>] Function: Show the current MAC table

Parameter: static static entry; **aging-time** address aging time; **discardiia** filter entry; **<*mac-addr*>** entry's MAC address; **<*vlan-id*>** entry's VLAN number; **<*interface-name*>** entry's interface name

Command mode: Admin mode

Default: MAC address table is not displayed by default.

Usage guide: This command can display various sorts of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

Example: Display all the filter MAC address entries.

Switch#show mac-address-table discardish

4.4.2 Troubleshooting Help

Using the show mac-address-table command, a port is found to be failed to learn the MAC of a device connected to it. Possible reasons:

- ☞ The connected cable is broken, replace the cable.
- ☞ Spanning Tree is started and the port is in "discarding" status; or the device is just connected to the port and Spanning Tree is still under calculation, wait until the Spanning Tree calculation finishes, and the port will learn the MAC address.
- ☞ If not the abovementioned problem, please check for port healthy and contact technical support for solution for port problems.

4.5 MAC Address Function Extension

4.5.1 MAC Address Binding

4.5.1.1 Introduction to MAC Address Binding

Most switches support MAC address learning, each port can dynamically learn several MAC addresses, so that forwarding data streams between known MAC addresses within the ports can be achieved. If a MAC address is aged, the packet destined for that entry will be broadcasted. In other words, a MAC address learned in a port will be used for forwarding in that port, if the connection is changed to another port, the switch will learn

the MAC address again to forward data in the new port.

However, in some cases, security or management policy may require MAC addresses to be bound with the ports, only data stream from the binding MAC are allowed to be forwarded in the ports. That is to say, after a MAC address is bound to a port, only the data stream destined for that MAC address can flow in from the binding port, data stream destined for the other MAC addresses that not bound to the port will not be allowed to pass through the port.

4.5.1.2 MAC Address Binding Configuration

4.5.1.2.1 MAC Address Binding Configuration Task Sequence

1. Enable MAC address binding function for the ports
2. Lock the MAC addresses for a port
3. MAC address binding property configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Interface Mode	
port securityno port-security	Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no switchport port-security"** command disables the MAC address binding function for the port**,**and restores the MAC address learning function for the port.

2. Lock the MAC addresses for a port

Command	Explanation
Interface Mode	
switchport port-security convert	Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses.

switchport port-security timeout <*value*> **no switchport port-security timeout**	Enable port locking timer function; the "**no switchport port-security timeout**" restores the default setting.
switchport port-security mac-address <*mac-address*> **no switchport port-security mac-address <*mac-address*>**	Add static secure MAC address; the "**no switchport port-security mac-address"** command deletes static secure MAC address.
Admin Mode	
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	Clear dynamic MAC addresses learned by the specified port.

3. MAC address binding property configuration

Command	Explanation
Interface Mode	
switchport port-security maximum <*value*> **no switchport port-security maximum <*value*>**	Set the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the default value.
port security actionshutdown **no port security violation**	Set the violation mode for the port; the "**no switchport port-security violation**" command restores the default setting.

4.5.1.2.2 MAC Address Binding Configuration Commands

4.5.1.2.2.1 port security

Command: port security

no port security

Function: Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no switchport port-security"** command disables the MAC address binding function for the port and restores the MAC address learning function for the port.

Command mode: Interface Mode

Default: MAC address binding is not enabled by default.

Usage Guide: The MAC address binding function, Spanning Tree and Port Aggregation functions are mutually exclusive. Therefore, if MAC binding function for a port is to be

enabled, the Spanning Tree and Port Aggregation functions must be disabled, and the port enabling MAC address binding must not be a Trunk port.

Example: Enable MAC address binding function for port 1and and lock the port. When a port is locked, the MAC address learning function for the port will be disabled.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#port security

4.5.1.2.2.2 switchport port-security convert

Command: switchport port-security convert

Function: Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses, and disables the MAC address learning function for the port.

Command mode: Interface Mode

Usage Guide: The port dynamic MAC convert command can only be executed after the secure port is locked. After this command is executed, the dynamic secure MAC addresses learned by the port will be converted to static secure MAC addresses. The command does not reserve configuration.

Example: Convert MAC addresses in port 1 to static secure MAC addresses.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security convert

4.5.1.2.2.3 switchport port-security timeout

Command: switchport port-security timeout <*value*>

no switchport port-security timeout

Function: Set the timer for port locking; the "**no switchport port-security timeout**" command restores the default setting.

Parameter: < *value*> is the timeout value, the valid range is 0 to 300s.

Command mode: Interface Mode

Default: Port locking timer is not enabled by default.

Usage Guide: The port locking timer function is a dynamic MAC address locking function. MAC address locking and conversion of dynamic MAC entries to secure address entries will be performed on locking timer timeout. The MAC address binding function must be enabled prior to running this command.

Example: Set port1 locking timer to 30 seconds.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# switchport port-security timeout 30

4.5.1.2.2.4 switchport port-security mac-address

Command: switchport port-security mac-address <*mac-address*>

no switchport port-security mac-address <*mac-address*>

Function: Add static secure MAC address; the "**no switchport port-security mac-address"** command deletes static secure MAC address.

Command mode: Interface Mode

Parameter: <*mac-address*> stands for the MAC address to be added/deleted.

Usage Guide: The MAC address binding function must be enabled before static secure MAC address can be added.

Example: Add MAC 00-03-0F-FE-2E-D3 to port1.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security mac-address 00-03-0F-FE-2E-D3

4.5.1.2.2.5 clear port-security dynamic

Command: clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]

Function: Clear the Dynamic MAC addresses of the specified port.

Command mode: Admin Mode

Parameter: <*mac-addr*> stands MAC address; **<*interface-id*>** for specified port number.

Usage Guide: The secure port must be locked before dynamic MAC clearing operation can be perform in specified port. If no ports and MAC are specified, then all dynamic MAC in all locked secure ports will be cleared; if only port but no MAC address is specified, then all MAC addresses in the specified port will be cleared.

Example: Delete all dynamic MAC in port1.

Switch#clear port-security dynamic interface Ethernet 1/1

4.5.1.2.2.6 switchport port-security maximum

Command: switchport port-security maximum <*value*>

no switchport port-security maximum

Function: Sets the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the maximum secure address number of 1.

Command mode: Interface Mode

Parameter: < *value*> is the up limit for static secure MAC address, the valid range is 1 to 128.

Default: The default maximum port secure MAC address number is 1.

Usage Guide: The MAC address binding function must be enabled before maximum secure MAC address number can be set. If secure static MAC address number of the port is larger than the maximum secure MAC address number set, the setting fails; extra secure static MAC addresses must be deleted, so that the secure static MAC address number is no larger than the maximum secure MAC address number for the setting to be successful.

Example: Set the maximum secure MAC address number for port 1 to 4.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security maximum 4

4.5.1.2.2.7 port security action shutdown

Command: port security actionshutdown

no port security action

Function: Set the violation mode for the port; the "**no**" command restores the violation mode to protect mode ..

Command mode: Interface Mode

Default: The default violation mode for the port "protect mode".

Usage Guide: The port violation mode can only be set after MAC address binding function is enabled. If the port violation mode is set to "protect mode", when the secure Mac address number exceeds maximum secure MAC address number set, only the dynamic MAC address learning ability is disabled; if the violation mode is set to "shutdown", then the port will be shutdown when the secure Mac address number exceeds maximum secure MAC address number set, the user can manually enable the port by "**no shutdown**" command.

Example: Set the violation mode for port1 to "**shutdown**".

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# port security action shutdown

4.5.1.3 Mac Address Binding Troubleshooting Help

4.5.1.3.1 MAC Address Binding Debug and Monitor Commands

4.5.1.3.1.1 show port-security

Command: show port-security

Function: display the global configuration of secure ports.

Command mode: Admin Mode

Default: Configuration of secure ports is not displayed by default.

Usage Guide: This command displays the information for ports that are currently configured as secure ports.

Example:

```
Switch#show port-security
Security Port       MaxSecurityAddr CurrentAddr       Security Action
                        (count)          (count)
-----------------------------------------------------------------------------------------------
 Ethernet1/3              128              0                 Protect
-----------------------------------------------------------------------------------------------
Max Addresses limit per port : 128
Total Addresses in System : 2
```

Displayed information	Explanation
Security Port	Name of port that is configured as a secure port.
MaxSecurityAddr	The maximum secure MAC address number set for the secure port.
CurrentAddr	Current secure MAC address number for the secure port.
Security Action	Violation mode set for the port.
Max Addresses limit per port	Maximum secure MAC address number set for each secure port.
Total Addresses in System	Current secure MAC address number in the system.

4.5.1.3.1.2 show port-security interface

Command: show port-security interface *<interface-id>*

Function: display the configuration of secure port.

Command mode: Admin Mode

Parameter: *<interface-list>* stands for the port to be displayed.

Default: Configuration of secure ports is not displayed by default.

Usage Guide: This command displays the detailed configuration information for the secure port.

Example:

Switch#show port-security interface ethernet 1/1

Ethernet1/1 Port Security : Enabled

Port status : Security Up

Violation mode : Protect

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Lock Timer is ShutDown

Mac-Learning function is : Closed

Displayed information	Explanation
Port Security :	Is port enabled as a secure port?
Port status:	Port secure status
Violation mode :	Violation mode set for the port.
Maximum MAC Addresses :	The maximum secure MAC address number set for the port
Total MAC Addresses :	Current secure MAC address number for the port.
Configured MAC Addresses :	Current secure static MAC address number for the port.
Lock Timer	Whether locking timer (timer timeout) is enabled for the port.
Mac-Learning function	Is the MAC address learning function enabled?

4.5.1.3.1.3 show port-security address

Command: show port-security address [interface <*interface-id*>]

Function: Display the secure MAC addresses of the port.

Command mode: Admin Mode

Parameter: <*interface-list*> stands for the port to be displayed.

Usage Guide: This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed. The following is an example:

Switch#show port-security address interface ethernet 1/3

Ethernet1/3 Security Mac Address Table

```
-------------------------------------------------------------------------------------------
Vlan      Mac Address              Type                      Ports
 1        0000.0000.1111           SecureConfigured          Ethernet1/3
-------------------------------------------------------------------------------------------
Total Addresses : 1
```

Displayed information	Explanation
Vlan	The VLAN ID for the secure MAC Address
Mac Address	Secure MAC address
Type	Secure MAC address type
Ports	The port that the secure MAC address belongs to
Total Addresses	Current secure MAC address number in the system.

4.5.1.3.2 MAC Address Binding Troubleshooting Help

Enabling MAC address binding for ports may fail in some occasions. Here are some possible causes and solutions:

- ☞ If MAC address binding cannot be enabled for a port, make sure the port is not executing Spanning tree, port aggregation and is not configured as a Trunk port. MAC address binding is exclusive to such configurations. If MAC address binding is to be enabled, the abovementioned functions must be disabled first.
- ☞ If a secure address is set as static address and deleted, than that secure address will be unusable even though it exists. For this reason, it is recommended to avoid static address for ports enabling MAC address binding.

4.6 WEB Management

Click MAC address table configuration. The MAC address configuration page is shown. Users can manage MAC addresses on the switch.

4.6.1 MAC address table configuration

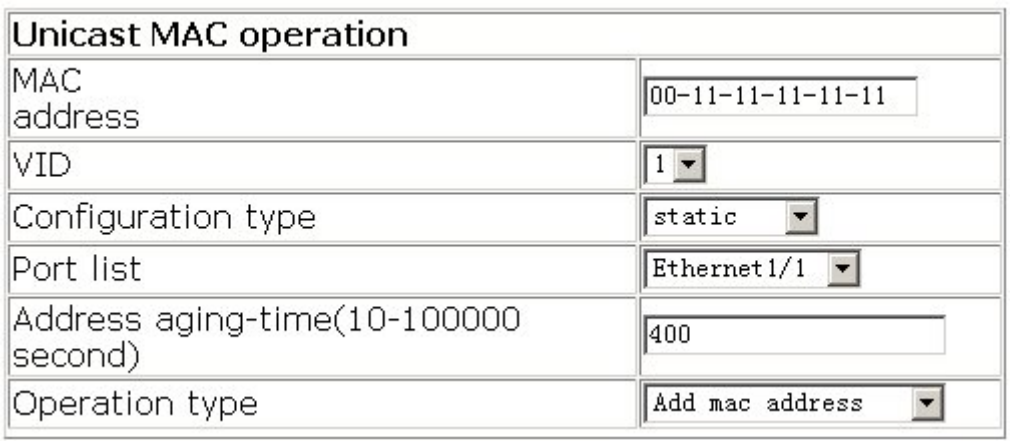
Click MAC address table configuration, MAC address table configuration. Users can manage, add and delete MAC addresses.

4.6.1.1 Unicast address configuration

Click MAC address table configuration, MAC address table configuration, Unicast address configuration. Users can add and delete MAC address. See the equivalent CLI command at 4.2.2:

- MAC address – Specify MAC address
- VID – Vlan number of the MAC address
- Configuration type – static; blackhole
- Port list – Port of the MAC address
- Address aging-time – MAC address aging-time
- Operation type – Add MAC address; delete MAC address

For example: Set MAC address to 00-11-11-11-11-11; Select VID to 1; select Configuration type to static; select Port list to Ethernet1/1; set Address aging-time to 400 seconds; select Operation type to add mac address, and then click Add. This configuration is to add static MAC address 00-11-11-11-11-11 to interface Ethernet 1/1 with VID of 1.

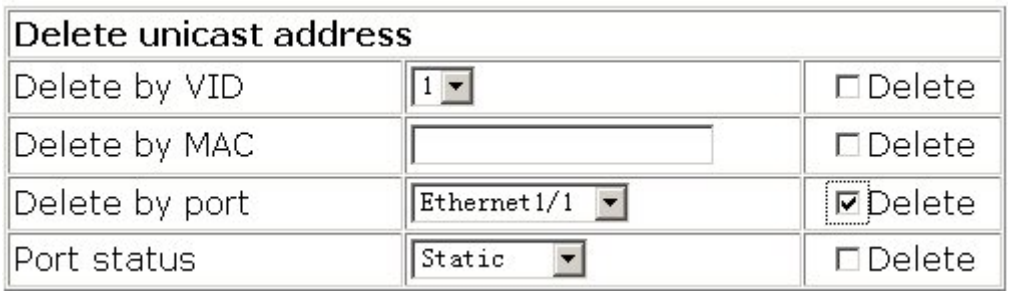


4.6.1.2 Remove static MAC address

Click MAC address table configuration, MAC address table configuration, Remove static MAC address. Users can delete MAC address. See the equivalent CLI command at 4.2.2:

- Delete by VID – Specify VID to delete static MAC address. Check “Delete” box to delete MAC address according to VID.
- Delete by MAC – Specify MAC address. Check “Delete” box to delete specified MAC address.
- Delete by port – Specify port to delete MAC address. Check “Delete” box to delete MAC address according to port.
- Port status – Static; dynamic; discard. Check “Delete” box to delete MAC address according to port MAC status.

For example: Select VID 1; select interface Ethernet1/1; select Port status to Static, and then click Apply. All the static MAC addresses on the interface Ethernet 1/1 are deleted.

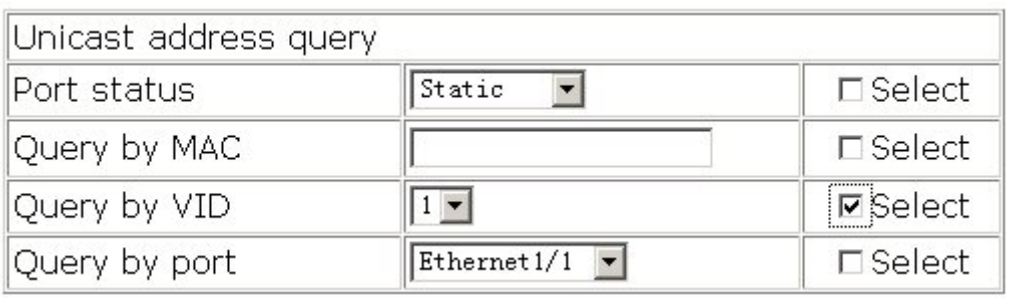


4.6.1.3 Static MAC query

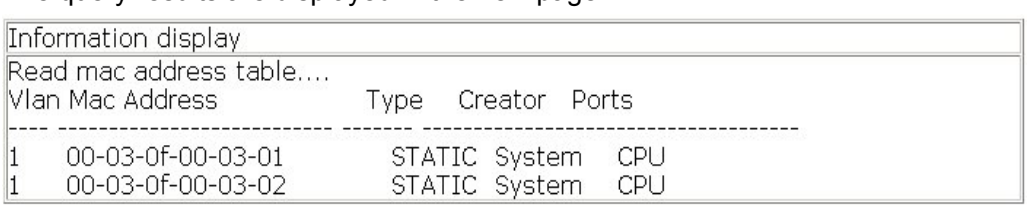
Click MAC address table configuration, MAC address table configuration, Static MAC query. Users can query MAC address. See the equivalent CLI command at 4.4.1.1:

- Query by VID – Specify VID to search static MAC address. Check “Search” box to search MAC address according to VID.
- Query by MAC –Search MAC address. Check “Search” box to search MAC address according to MAC address typed.
- Query by port – Specify port to search MAC address. Check “Search” box to search MAC address according to port.
- Port status – Static; dynamic; discard. Check “Search” box to search MAC address according to port MAC status.

For example: Select Port status; check “Port status” box, and then click Search.



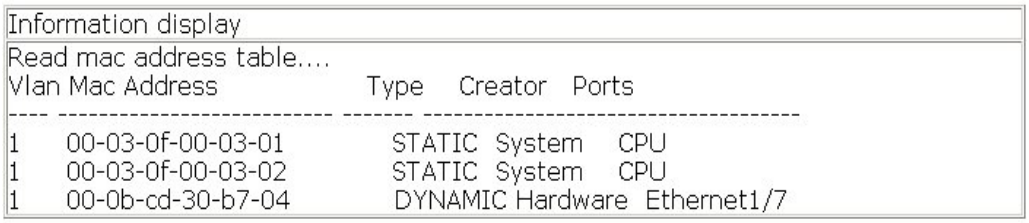
The query results are displayed in the new page.


Information display
Read mac address table....
Vlan Mac Address Type Creator Ports
1 00-03-0f-00-03-01 STATIC System CPU
1 00-03-0f-00-03-02 STATIC System CPU

4.6.1.4 Show mac-address-table

Click MAC address table configuration, MAC address table configuration, show

mac-address-table. The current MAC address information is shown. See the equivalent CLI command at 4.4.1.1:


Information display
Read mac address table....
Vlan Mac Address Type Creator Ports
1 00-03-0f-00-03-01 STATIC System CPU
1 00-03-0f-00-03-02 STATIC System CPU
1 00-0b-cd-30-b7-04 DYNAMIC Hardware Ethernet1/7

4.6.2 MAC address table configuration

Click MAC address table configuration, MAC address binding configuration. Users can configure secure port features.

4.6.2.1 Enbale port Mac-binding

Click MAC address table configuration, MAC address binding configuration, Enbale port Mac-binding. Users can configure secure port features.

4.6.2.1.1 Enbale port Mac-binding

Click MAC address table configuration, MAC address binding configuration, Enable port Mac-binding, Enable port Mac-binding. Users can enable or disable switch port MAC binding. See the equivalent CLI command at 4.5.1.2.2.1

- Port – Specify port

For example: Select port Ethernet1/1, and then click Apply. The MAC address binding is enabled on the port Ethernet1/1.



4.6.2.2 Lock port

Click MAC address table configuration, MAC address binding configuration, Lock port. Users can lock the secure port and configure MAC address converting.

4.6.2.2.1 Lock port

Click MAC address table configuration, MAC address binding configuration, Lock port,

Lock port. User can lock the secure port. See the equivalent CLI command at 4.5.1.2.2.3

- ☞ Port – Specify port

For example: Select port Ethernet1/1, and then click Apply. The port Ethernet1/1 is locked. Click Remove to disable port MAC address binding.

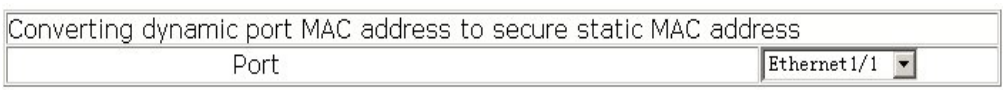


4.6.2.2.2 Dynamic MAC converting

Click MAC address table configuration, MAC address binding configuration, Lock port, Dynamic MAC converting. Users can convert the MAC address which is learned dynamically to secure static IP address. See the equivalent CLI command at 4.5.1.2.2.2.

- ☞ Port – Specify the port

For example: Select port Ethernet1/1, and then click Apply. The dynamic MAC address of port Ethernet1/1 is converted to the secure static address. Click Reset to select the new port

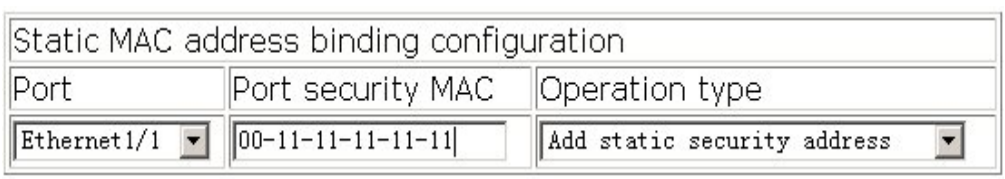


4.6.2.2.3 Enable port security timeout

Click MAC address table configuration, MAC address binding configuration, Lock port, Enable port security timeout. Users can lock the secure port. See the equivalent CLI command at 4.5.1.2.2.4:

- ☞ Port – Specify the port
- ☞ Timeout Value (0-300 second) – Security timeout value

For example: Select port Ethernet1/1; set Timeout Value to 30 seconds, and then click Apply. The security timeout value of port Ethernet1/1 is 30 second.



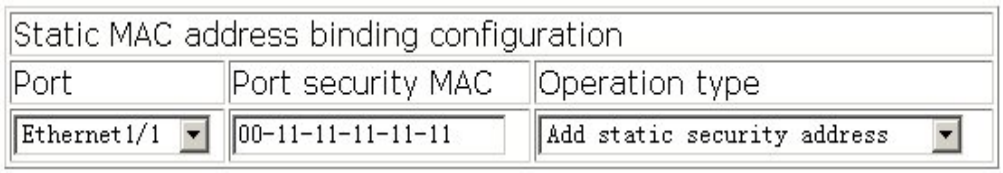
4.6.2.2.4 Binding MAC

Click MAC address table configuration, MAC address binding configuration, Lock port, Binding MAC. Users can add and delete secure static MAC address. See the equivalent

CLI command at 4.5.1.2.2.5:

- Port – Specify the port
- Port security MAC –Port security MAC address
- Operation type – add static security address; Remove static security address

For example: Select port Ethernet1/1; set MAC address to 00-11-11-11-11-11; Select add static security address, and then click Apply. The configuration is applied on the switch.

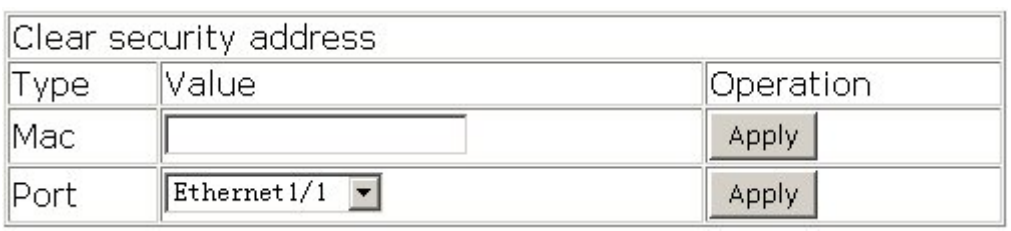


4.6.2.2.5 Clearing port MAC

Click MAC address table configuration, MAC address binding configuration, Lock port, Clearing port MAC. Users can clear the dynamic MAC address of the specified port. See the equivalent CLI command at 8.5.1.2.2.6:

- Mac – Specify the MAC
- Port – Specify the port

For example: Select port Ethernet1/1, and then click Apply. The MAC address of the port Ethernet1/1 is deleted. Note: This feature is only supported on the secure port.



4.6.2.3 MAC binding attribution configuration

Click MAC address table configuration, MAC address binding configuration, MAC binding attribution configuration. Users can configure secure port attributes.

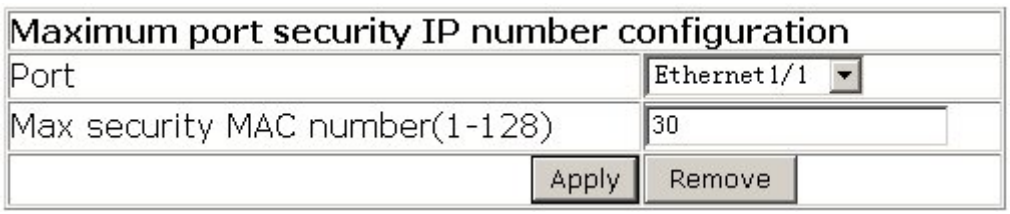
4.6.2.3.1 Maximum port security IP number configuration

Click MAC address table configuration, MAC address binding configuration, MAC binding attribution configuration, Maximum port security IP number configuration. Users can configure maximum port security IP number. See the equivalent CLI command at

4.5.1.2.2.7

- Port – Specify the port
- Max security MAC number (1-128) – Maximum MAC number

For example: Select port Ethernet1/1; set Max security MAC number to 30, and then click Apply. The configuration is applied on the switch. Click Remove to restore the default setting.

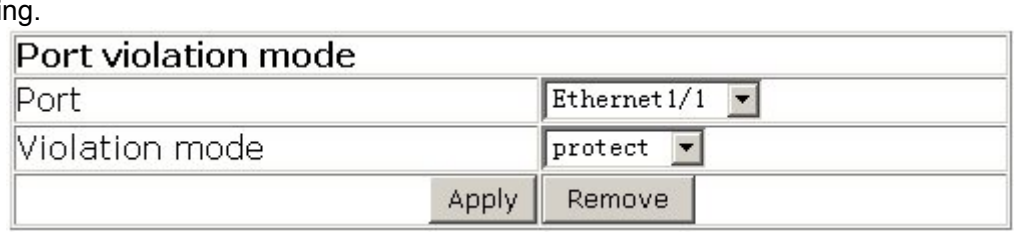


4.6.2.3.2 Port violation mode

Click MAC address table configuration, MAC address binding configuration, MAC binding attribution configuration, Port violation mode. Users can configure port violation mode. See the equivalent CLI command at 4.5.1.2.2.8:

- Port – Specify the port
- Violation mode – Set violation mode: protect mode or shutdown mode

For example: Select port Ethernet1/1; set Violation mode to protect, and then click Apply. The configuration is applied on the switch. Click Remove to restore the default setting.



4.6.2.4 MAC binding debug

Click MAC address table configuration, MAC address binding configuration, MAC binding debug. Users can view secure port debug information.

4.6.2.4.1 Port binding MAC information query

Click MAC address table configuration, MAC address binding configuration, MAC binding debug, Port binding MAC information query. Users can query the secure port information:

- Show port-security by interface – Show specified secure MAC address. See the equivalent CLI command at 4.5.1.3.1.2
- Show port-security address by interface – Show the secure MAC address of the

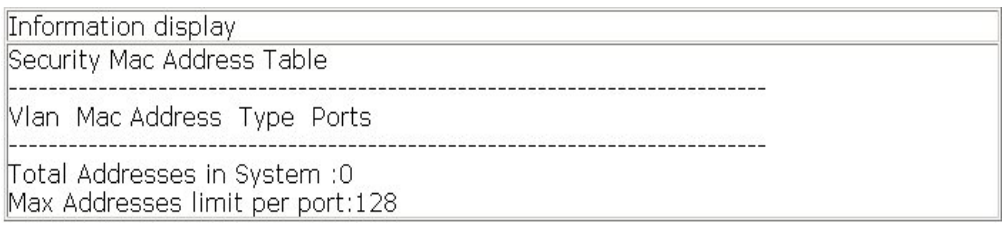
specified port. See the equivalent CLI command at 4.5.1.3.1.3

- Show all port-security – Show secure port configuration. See the equivalent CLI command at 8.5.1.3.1.1
- Show all port-security address – Show secure port MAC address. See the equivalent CLI command at 4.5.1.3.1.3

Click Show Port Configuration. The security configuration is shown.



The results are shown in Information Display window:


Information display
Security Mac Address Table
Vlan Mac Address Type Ports
Total Addresses in System :0
Max Addresses limit per port:128

Chapter 5 VLAN Configuration

5.1 Introduction to VLAN

VLAN (Virtual Local Area Network) is a technology that divides the logical addresses of devices within the network to separate network segments basing on functions, applications or management requirements. This way, virtual workgroups can be formed regardless of the physical location of the devices. IEEE announced IEEE 802.1Q protocol to direct the standardized VLAN implementation, and the VLAN function of ES4626/ES4650 is implemented following IEEE 802.1Q.

The characteristics of VLAN technology is a big LAN can be partitioned into many separate broadcast domains dynamically to meet the demands.

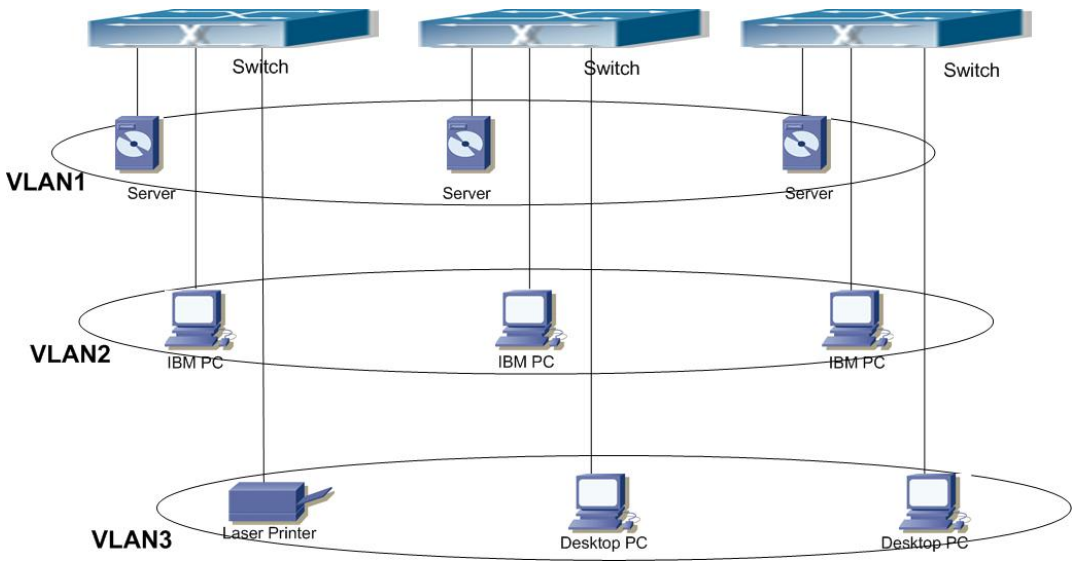


Fig 5-1 A VLAN network defined logically

Each broadcast domain is a VLAN. VLANs have the same properties as the physical LANs, except VLAN is a logical partition rather than physical one. Therefore, the partition of VLANs can be performed regardless of physical locations, and the broadcast, multicast and unicast traffic within a VLAN is separated from the other VLANs.

With the aforementioned features, VLAN technology provides us with the following convenience:

- Improving network performance
- Saving network resources
- Simplifying Network Management
- Lowering network cost

- Enhancing network security

VLAN and GVRP (GARP VLAN Registration Protocol) defined by 802.1Q are implemented in ES4626/ES4650. The chapter will describe the use and configuration of VLAN and GVRP in details.

5.2 VLAN Configuration

5.2.1 VLAN Configuration Task Sequence

1. Creating or deleting VLAN
2. Specifying or deleting VLAN name
3. Assigning Switch ports for VLAN
4. Set the port type for the switch
5. Set Trunk port
6. Set Access port
7. Enable/Disable VLAN ingress rules on ports

1. Creating or deleting VLAN

Command	Explanation
Global Mode	
vlan <*vlan-id*> [name <*vlan-name*>] **no vlan <*vlan-id*>[name]**	Create/delete VLAN or enter VLAN Mode and Set or delete VLAN name

2. Assigning Switch ports for VLAN

Command	Explanation
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Assign Switch ports to VLAN

3. Set The Switch Port Type

Command	Explanation
Interface Mode	
switchport mode {trunk|access}	Set the current port as Trunk or Access port.

4. Set Trunk port

Command	Explanation
Interface Mode	
Switchport allowedvlan {add<*vlan-list*>| remove <*vlan-list*>} **no switchport allowed vlan**	Set/delete VLAN allowed to be crossed by Trunk. The "no". command restores the default setting.
switchport native vlan <*vlan-id*> **no switchport native vlan**	Set/delete PVID for Trunk port.

5. Set Access port

Command	Explanation
Interface Mode	
switchport allowed add vlan <*vlan-id*> **no switchport access vlan**	Add the current port to specified VLAN the specified VLANs. The "no". command restores the default setting.

6. Disable/Enable VLAN Ingress Rules

Command	Explanation
Global Mode	
switchport ingress-filteringno switchport ingress-filtering	Disable/Enable VLAN ingress rules

7. Configure Private VLAN

Command	Explanation
VLAN mode	
private-vlan {primary|isolated|community} **no private-vlan**	Configure current VLAN to Private VLAN

8. Set Private VLAN association

Command	Explanation
VLAN mode	
private-vlan association <*secondary-vlan-list*> **no private-vlan association**	Set/delete Private VLAN association

5.2.2VLAN Configuration Commands

5.2.2.1 vlan

Command: vlan <*vlan-id*>[name <*vlan-name*>]

no vlan <*vlan-id*>[name]

Function: Create a VLAN and enter VLAN configuration mode, and can set VLAN name. In VLAN Mode, the user can assign the switch port to the VLAN. The "**no vlan <*vlan-id*>**" command deletes specified VLANs.

Parameter: <*vlan-id*> is the VLAN ID to be created/deleted, valid range is 1 to 4094.

<*vlan-name*> is the name that **create VLAN,** valid range is 1 to 16 characters

Command mode: Global Mode

Default: Only VLAN1 is set by default.

Usage Guide: VLAN1 is the default VLAN and cannot be configured or deleted by the user. The allowed VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.

Example: Create VLAN100 and enter the configuration mode for VLAN 100.

Switch(Config)#vlan 100

Switch(Config-Vlan100)#

5.2.2.2 switchport access vlan

Command: switchport access vlan <*vlan-id*>

no switchport access vlan

Function: Add the current Access port to the specified VLAN, the "**no switchport access vlan**" command delete the current port from the specified VLAN, and the port will be partitioned to VLAN1.

Parameter: <*vlan-id*> is the VID for the VLAN to add current port, valid range is 1 to 4094.

Command mode: Interface Mode

Default: All ports belong to VLAN1 by default.

Usage Guide: Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

Example: Add some Access port to VLAN100.

Switch(Config)#interface ethernet 1/8

Switch(Config-ethernet1/8)#switchport mode access
Switch(Config-ethernet1/8)#switchport access vlan 100
Switch(Config-ethernet1/8)#exit

5.2.2.3 switchport interface

Command: switchport interface <*interface-list*>

no switchport interface <*interface-list*>

Function: Specify Ethernet port to VLAN; the "**no switchport interface <*interface-list*>**" command deletes one or one set of ports from the specified VLAN.

Parameter: **<*interface-list*>** is the port list to be added or deleted, ";" and "-" are supported, for **example:** ethernet 1/1;2;5 or ethernet 1/1-6;8.

Command mode: VLAN Mode

Default: A newly created VLAN contains no port by default.

Usage Guide: Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

Example: Assign Ethernet port 1, 3, 4-7, 8 of slot 1 to VLAN100.

Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8

5.2.2.4 switchport mode

Command: switchport mode {trunk|access}

Function: Set the port in access mode or trunk mode.

Parameter: trunk means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only.

Command mode: Interface Mode

Default: The port is in Access mode by default.

Usage Guide: Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through, VLAN in different switches can be interconnected with the Trunk ports interconnections. Ports under access mode is called Access ports. An access port can be assigned to one and only one VLAN at a time.

Example: Set port 1/5 to trunk mode and port 1/8 to access mode.

Switch(Config)#interface ethernet 1/5

Switch(Config-ethernet1/5)#switchport mode trunk
Switch(Config-ethernet1/5)#exit
Switch(Config)#interface ethernet 1/8

Switch(Config-ethernet1/8)#switchport mode access
Switch(Config-ethernet1/8)#exit

5.2.2.5 switchport trunk allowed vlan

Command: switchport trunk allowed vlan {<*vlan-list*>|all}

no switchport trunk allowed vlan

Function: Set trunk port to allow VLAN traffic; the "**no switchport trunk allowed vlan**" command restores the default setting.

Parameter: <*vlan-list*> is the list of VLANs allowed to pass through in the specified Trunk port; keyword "**all"** indicate allow all VLAN traffic on the Trunk port.

Command mode: Interface Mode

Default: Trunk port allows all VLAN traffic by default.

Usage Guide: The user can use this command to set the VLAN traffic allowed to pass though the trunk port; traffic of VLANs not included are prohibited.

Example: Set Trunk port to allow traffic of VLAN1, 3, 5-20.

Switch(Config)#interface ethernet 1/5
Switch(Config-ethernet1/5)#switchport mode trunk
Switch(Config-ethernet1/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-ethernet1/5)#exit

5.2.2.6 switchport trunk native vlan

Command: switchport trunk native vlan <*vlan-id*>

no switchport trunk native vlan

Function: Set the PVID for Trunk port; the "**no switchport trunk native vlan**" command restores the default setting.

Parameter: <*vlan-id*> is the PVID for Trunk port.

Command mode: Interface Mode

Default: The default PVID of Trunk port is 1.

Usage Guide: PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When a untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this command for VLAN forwarding.

Example: Set the native vlan for a Trunk port to 100.

Switch(Config)#interface ethernet 1/5
Switch(Config-ethernet1/5)#switchport mode trunk
Switch(Config-ethernet1/5)#switchport trunk native vlan 100

Switch(Config-ethernet1/5)#exit

5.2.2.7 switchport ingress-filtering

Command: switchport ingress-filtering

no switchport ingress-filtering

Function: Enable the VLAN ingress rule for a port; the "**no vlan ingress disable**" command disable the ingress rule.

Command mode: Interface Mode

Default: VLAN ingress rules are enabled by default.

Usage Guide: When VLAN ingress rules are enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is a VLAN member port.

Example: Disable VLAN ingress rules on the port

Switch(Config-Ethernet1/1)# no switchport ingress-filtering

5.2.2.8 private-vlan

Command: private-vlan

no private-vlan

Function: Set the current VLAN to Private VLAN; the "**no private-vlan**" command cancels Private VLAN.

Parameter: primary sets the current VLAN to Primary VLAN; **isolated** sets the current VLAN to Isolated VLAN; **community** sets the current VLAN to Community VLAN.

Command mode: VLAN Mode

Usage Guide: There are three types of VLANs: Primary VLAN, Isolated VLAN and Community VLAN. The ports in Primary VLAN can communicate with the ports in Isolated VLAN and Community VLAN which are associated to the Primary VLAN; the ports in Isolated VLAN can't communicate each other. They can only communicate to the ports in the associated Primary VLAN; the ports in Community VLAN can communicate each other and they can also communicate to the ports in the associated Primary VLAN. The ports in Isolated VLAN can't communicate to the ports in Community VLAN.

Only the VLAN which doesn't have any member ports can be set to Private VLAN; only the Private VLAN which has already configured association relationship can add Access ports as its member ports; when the VLAN is set to Private VLAN, all the member ports are removed from the VLAN.

Note: The ports in Isolated VLAN must be configured by the command: **no switchport ingress-filtering**; GVRP can't transmit Private VLAN information.

Example: Set VLAN100, VLAN200 and VLAN300 to Private VLAN. Set VLAN100 to Primary VLAN; set VLAN200 to Isolated VLAN; set VLAN300 to Community VLAN.

5.2.2.9 private-vlan association

Command: private-vlan association

no private-vlan association

Function: Set Private VLAN association; the "**no private-vlan association**" command cancels Private VLAN association.

Parameter: <*secondary-vlan-list*> Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLAN by ";".

Command mode: VLAN Mode

Default: There is no Private VLAN association by default.

Usage Guide: This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN. Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN which has Private VLAN association can't be deleted; when users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

Example: Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

Switch(Config-Vlan100)#private-vlan association 200;300

5.2.3 Typical VLAN Application

Scenario:

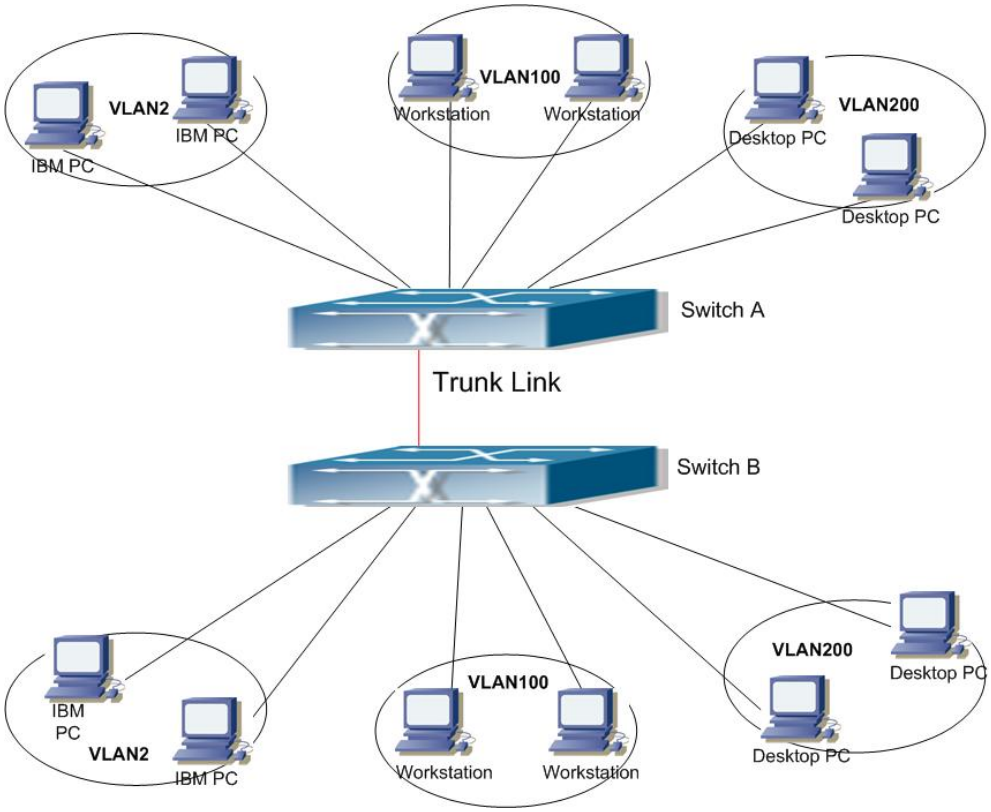


Fig 5-2 Typical VLAN Application Topology

The existing LAN is required to be partitioned to 3 VLANs due to security and application requirements. The three VLANs are VLAN2, VLAN100 and VLAN200. Those three VLANs must cross location A and B. One switch is placed in each site, and cross-location requirement can be met if VLAN traffic can be transferred between the two switches.

Configuration Item	Configuration description
VLAN2	Site A and site B switch port 2 – 4.
VLAN100	Site A and site B switch port 5 – 7.
VLAN200	Site A and site B switch port 8 – 10.
Trunk port	Site A and site B switch port 11 .

Connect the Trunk ports of both switch for a Trunk link to convey the cross-switch VLAN traffic; connect all network devices to the other ports of corresponding VLANs.
In this example, port 1 and port 12 is spared and can be used for management port or for other purposes.

The configuration steps are listed below:

Switch A:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
Switch(Config)#
```

Switch B:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
```

5.3 GVRP Configuration

GARP (Generic Attribute Registration Protocol) can be used to dynamically distribute, populate and register property information between switch members within a switch network, the property can be VLAN information, Multicast MAC address of the other information. As a matter of fact, GARP protocol can convey multiple property features the switch need to populate. Various GARP applications are defined on the basis of GARP, which are called GARP application entities, and GVRP is one of them.

GVRP (GARP VLAN Registration Protocol) is an application based on GARP working mechanism. It is responsible for the maintenance of dynamic VLAN register information

and population of such register information to the other switches. Switches support GVRP can receive VLAN dynamic register information from the other switches, and update local VLAN register information according the information received. GVRP enabled switch can also populate their won VLAN register information to the other switches. The VLAN register information populated includes local static information manually configured and dynamic information learnt from the other switches. Therefore, by populating the VLAN register information, VLAN information consistency can be achieved among all GVRP enabled switches.

5.3.1 GVRP Configuration Task Sequence

1. Configuring GARP Timer Parameters.
2. Enable GVRP function

1. Configuring GARP Timer parameters.

Command	Explanation
Interface Mode	
garp timer join <*timer-value*> **no garp timer join** **garp timer leave <*timer-value*>** **no garp timer leave** **garp timer hold <*timer-value*>** **no garp timer hold**	Configure the hold, join and leave timers for GARP.
Global Mode	
garp timer leave all <*timer-value*> **no garp timer leave all**	Configure the leave all timer for GARP.

2. Enable GVRP function

Command	Explanation
Interface Mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable the GVRP function on current port.
Global Mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable the GVRP function for the switch.

5.3.2 GVRP Commands

5.3.2.1 garp timer join

Command: garp timer join <*timer-value*>

no garp timer join

Function: Set the **join** timer for GARP; the " **no garp timer join**" command restores the default timer setting.

Parameter: < *timer-value*> is the value for **join** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **join** timer is 200 ms.

Usage Guide: GARP application entity sends a **join** message after **join** time timeout, other GARP application entities will register this message sent by this GARP application entity on receiving the **join** message.

Example: Set the GARP **join** timer value of port 1/10 to 1000 ms.

Switch(Config-Ethernet1/10)#garp timer join 1000

5.3.2.2 garp timer leave

Command: garp timer leave <*timer-value*>

no garp timer leave

Function: Set the **leave** timer for GARP; the " **no garp timer leave**" command restores the default timer setting.

Parameter: < *timer-value*> is the value for **leave** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **leave** timer is 600 ms.

Usage Guide: When GARP application entity wants to cancel a certain property information, it sends a **leave** message. GARP application entities receiving this message will start the **leave** timer, if no **join** message is received before **leave** timer timeout, the property information will be canceled. Besides, the value of **leave** timer must be larger than twice of **join** timer, otherwise a error message will be displayed.

Example: Set the GARP **leave** timer value of port 1/10 to 3000 ms.

Switch(Config-Ethernet1/10)#garp timer leave 3000

5.3.2.3 garp timer hold

Command: garp timer hold <*timer-value*>

no garp timer hold

Function: Set the **hold** timer for GARP; the " **no garp timer** hold" command restores the default timer setting.

Parameter: < *timer-value*> is the value for GARP **hold** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **hold** timer is 100 ms.

Usage Guide: When GARP application entities receive a **join** message, **join** message will not be sent immediately. Instead, **hold** timer is started. After **hold** timer timeout, all **join** messages received with the hold time will be sent in one GVRP frame, thus effectively reducing protocol message traffic.

Example: Set the GARP **hold** timer value of port 1/10 to 500 ms.

Switch(Config-Ethernet1/10)#garp timer hold 500

5.3.2.4 garp timer leaveall

Command: garp timer leaveall <*timer-value*>

no garp timer leaveall

Function: Set the **leaveall** timer for GARP; the " **no garp timer leaveall**" command restores the default timer setting.

Parameter: < *timer-value*> is the value for GARP **leaveall** timer, the valid range is 100 to 327650 ms.

Command mode: Global Mode

Default: The default value for **leaveall** timer is 10000 ms.

Usage Guide: When a GARP application entity starts, the **leaveall** timer is started at the same time. When **leaveall** timer timeout, the GARP application entity will send a **leaveall** message. Other application entities will cancel all property information for that application entity, and the **leaveall** timer is cleared for a new cycle.

Example: Set the GARP **leaveall** timer value to 50000 ms.

Switch(Config)#garp timer leaveall 50000

5.3.2.5 bridge-ext gvrp

Command: bridge-ext **gvrp**

no bridge-ext **gvrp**

Function: Enable the GVRP function for the switch or the current Trunk port; the "**no gvrp"** command disables the GVRP function globally or for the port**.**

Command mode: Interface Mode and Global Mode.

Default: GVRP is disabled by default.

Usage Guide: Port GVRP can only be enabled after global GVRP is enabled. When global GVRP is disabled, port GVRP configurations also void. Note GVRP can only be enabled on Trunk ports.

Example: Enable the GVRP function globally and for Trunk port 1/10.

Switch(Config)# **bridge-ext** gvrp

Switch(Config)#interface ethernet 1/10

Switch(Config-Ethernet1/10)# **bridge-ext** gvrp

Switch(Config)#exit

5.3.3 Typical GVRP Application

Scenario:

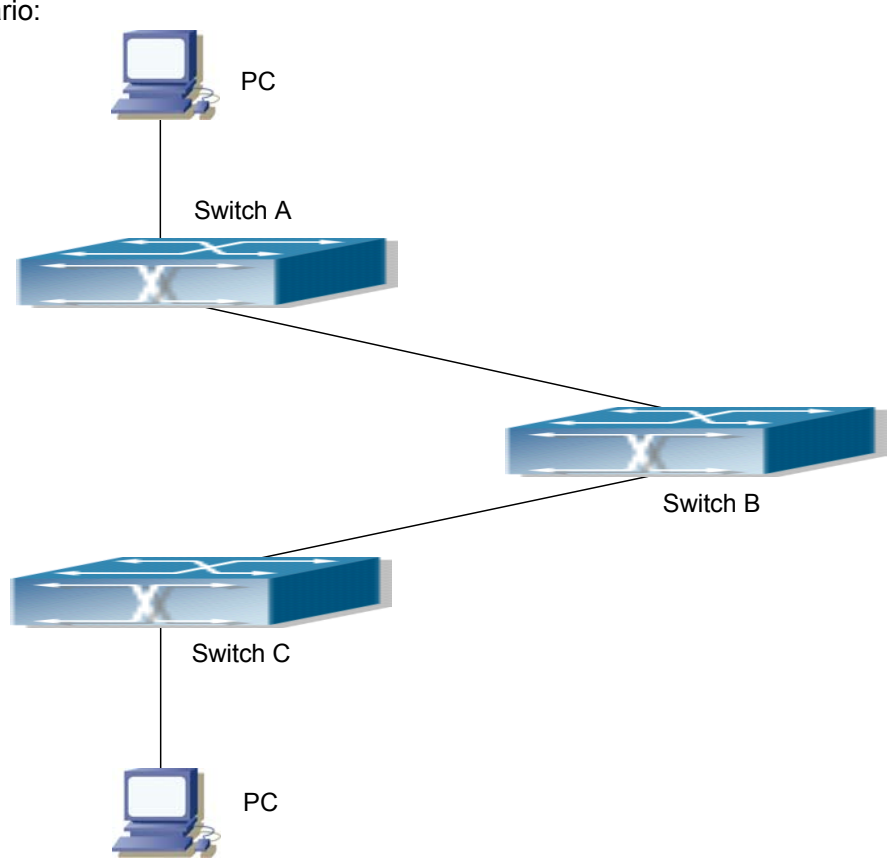


Fig 5-3 Typical GVRP Application Topology

To enable dynamic VLAN information register and update among switches, GVRP protocol is to be configured in the switch. Configure GVRP in Switch A, B and C, enable Switch B to learn VLAN100 dynamically so that the two workstation connected to VLAN100 in Switch A and C can communicate with each other through Switch B without static VLAN100 entries.

Configuration Item	Configuration description
VLAN100	Port 2 – 6 of Switch A and C
Trunk port	Port 11 of Switch A and C, Port 10, 11 of Switch B
Global GVRP	Switch A, B, C:
Port GVRP	Port 11 of Switch A and C, Port 10, 11 of Switch B

Connect the two workstation to the VLAN100 ports in switch A and B, connect port 11 of Switch A to port 10 of Switch B, and port 11 of Switch B to port 11 of Switch C. All ports are on slots 1 of Switch A, B and C.

The configuration steps are listed below:

Switch A:

```
Switch(Config)# bridge-ext gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(Config)#interface Ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit
```

Switch B:

```
Switch(Config)# bridge-ext gvrp
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)# bridge-ext gvrp
Switch(Config-Ethernet1/10)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit
```

Switch C:

Switch(Config)# bridge-ext gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit

5.4 VLAN Troubleshooting Help

5.4.1 Monitor and Debug Information

5.4.1.1 show vlan

Command: show vlan [brief| summary] [id <*vlan-id*>] [name <*vlan-name*>]
Function: Display detailed information for all VLANs or specified VLAN.
Parameter: brief stands for brief information; **summary** for VLAN statistics; ***<vlan-id>*** for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; ***<vlan-name>*** is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.
Command mode: Admin Mode
Usage Guide: If no ***<vlan-id>*** or ***<vlan-name>*** is specified, then information for all VLANs in the switch will be displayed.
Example: Display the status for the current VLAN; display statistics for the current VLAN.
Switch#show vlan

VLAN	Name	Type	Media	Ports
1	default	Static	ENET	Ethernet1/1 Ethernet1/2
				Ethernet1/3 Ethernet1/4
				Ethernet1/9 Ethernet1/10
				Ethernet1/11 Ethernet1/12
2	VLAN0002	Static	ENET	Ethernet1/5 Ethernet1/6
				Ethernet1/7 Ethernet1/8

Switch#sh vlan summary

The max. vlan entrys: 4094

Universal Vlan:
1 2
Total Existing Vlans is: 2

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN property, of statically configured or dynamically leaned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN
Universal Vlan	Universal VLAN.
Dynamic Vlan	Dynamic VLAN (not shown in this example)

5.4.1.2 show garp timer

Command: show garp timer [<*interface-name*>]
Function: Display the global and port information for GARP.
Parameter: <*interface-nam*> stands for the name of the Trunk port to be displayed.
Command mode: Admin Mode
Usage Guide: N/A.
Example: Display global GARP information.
Switch #show garp timer

5.4.1.3 show gvrp configuration

Command: show gvrp configuration [<*interface-name*>]
Function: Display the global and port information for GVRP.
Parameter: <*interface-nam*> stands for the name of the Trunk port to be displayed.
Command mode: Admin Mode
Usage Guide: N/A.
Example: Display global GVRP information.
Switch#show gvrp configuration
---------- Gvrp Information ----------
Gvrp status : enable

Gvrp Timers(milliseconds)
LeaveAll : 10000

5.4.1.4 debug gvrp

Command: debug gvrp
no debug gvrp
Function: Enable the GVRP debug function: the " no debug gvrp**"** command disables this debug function**.**
Command mode: Admin Mode
Default: GVRP debug information is disabled by default.
Usage Guide: Use this command to enable GVRP debug, GVRP packet processing information can be displayed.
Example: Enable GVRP debug.
Switch#debug gvrp

5.4.2 VLAN Troubleshooting Help

☞ The GARP counter setting in for Trunk ports in both ends of Trunk link must be the same, otherwise GVRP will not work properly.

It is recommended to avoid enabling GVRP and RSTP at the same time in ES4626/ES4650. If GVRP is to be enabled, RSTP function for the ports must be disabled first.

5.5 WEB Management

Click Vlan configuration. The Vlan configuration page is shown. User can configure the vlan information on the switch.

5.5.1 Vlan configuration

Click Vlan configuration, Vlan configuration. Users can configure the vlan information on the switch.

5.5.1.1 Create/Remove VLAN

Click Vlan configuration, Vlan configuration, Create/Remove VLAN. User can add or remove vlan.

5.5.1.1.1 VID allocation

Click Vlan configuration, Vlan configuration, Create/Remove VLAN, VID allocation. Users can add or remove vlan. See the equivalent CLI command at 5.2.2.1:

Operation type – Add new VID: Add a new vlan; Remove: Remove a vlan

VID – Specify VLAN ID

For example: Select Add new VID; set VID to 100, and then click Apply. The new VLAN 100 is created.



The current VLAN information is shown in VLAN ID information window:

VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan
2	VLAN0002	universal vlan

5.5.1.1.2 VID attribution configuration

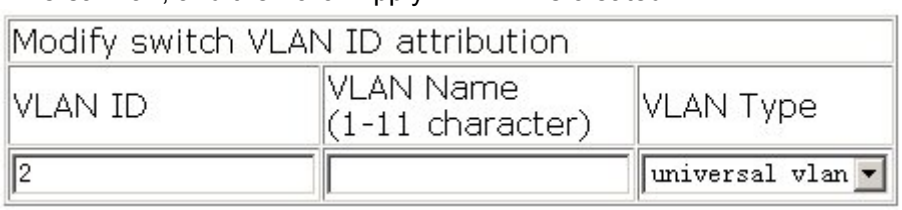
Click Vlan configuration, Vlan configuration, Create/Remove VLAN, VID attribution configuration. Users can configure VLAN attributes:

VLAN ID – Specify VLAN ID

VLAN Name – Set VLAN name. See the equivalent CLI command at 5.2.2.2

VLAN Type – Set VLAN type

For example: Set VLAN ID to; set VLAN Name to the default value; select VLAN Type to universal vlan, and then click Apply. VLAN 2 is created.



The current VLAN information is shown in VLAN ID information window:

VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan
2	VLAN0002	universal vlan

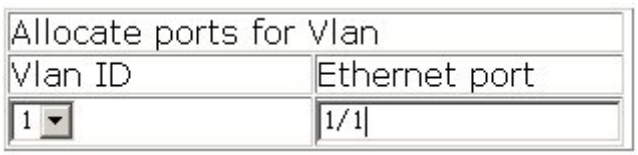
5.5.1.2 Allocate port for Vlan

Click Vlan configuration, Vlan configuration, Allocate ports for VLAN. Users can configure the vlan information on the switch.

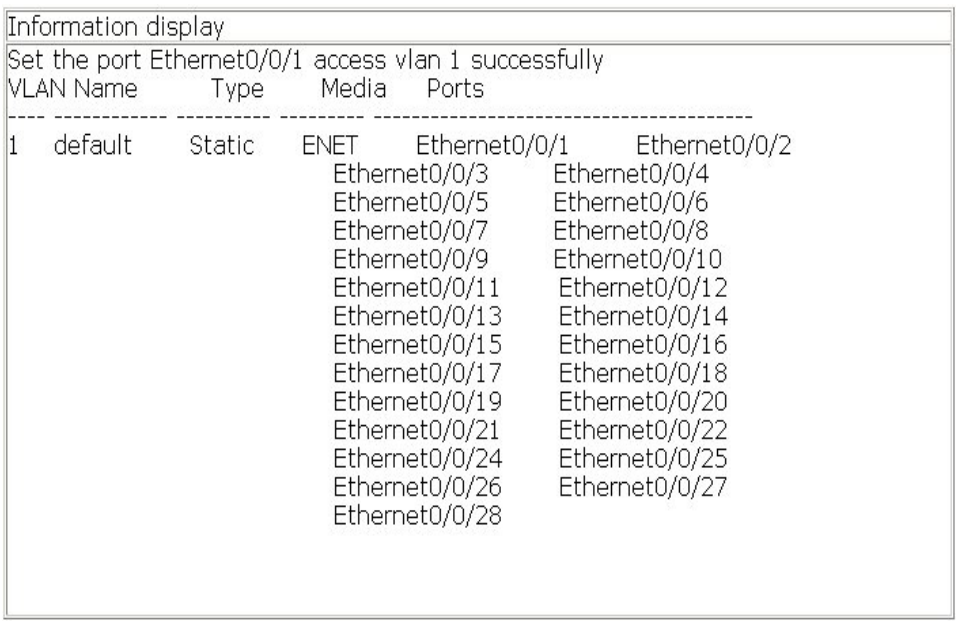
5.5.1.2.1 Allocate port for Vlan

Click Vlan configuration, Vlan configuration, Allocate ports for VLAN, Allocate port for Vlan. Users can add Ethernet ports to VLAN. See the equivalent CLI command at 5.2.2.4

For example: Select VLAN ID as 1; set Port to 1/1, and then click Apply. Ethernet 1/1 is added to VLAN 1.



The current VLAN information is shown in VLAN ID information window:



5.5.1.3 Port type configuration

Click Vlan configuration, Vlan configuration, Port type configuration. Users can configure port type.

5.5.1.3.1 Set port mode(Trunk/Access)

Click Vlan configuration, Vlan configuration, Port type configuration, Set port mode(Trunk/Access). Users can configure the port mode:

Port – Specify the port

Type – Specify port type: access, trunk. See the equivalent CLI command at 5.2.2.5

Vlan ingress rules – Enable or disable vlan ingress rule. See the equivalent CLI command at 5.2.2.8

For example: Select port Ethernet1/1; select Type to Trunk; select Enable Vlan ingress rules, and then click Apply. The configuration is applied on the switch.



The port mode information is shown in Port mode configuration window:

Port mode configuration	
Port	Type
Ethernet0/0/1	access
Ethernet0/0/2	access
Ethernet0/0/3	access
Ethernet0/0/4	access
Ethernet0/0/5	access
Ethernet0/0/6	access
Ethernet0/0/7	access
Ethernet0/0/8	access
Ethernet0/0/9	access
Ethernet0/0/10	access
Ethernet0/0/11	access
Ethernet0/0/12	access
Ethernet0/0/13	access
Ethernet0/0/14	access
Ethernet0/0/15	access

5.5.1.4 Trunk port configuration

Click Vlan configuration, Vlan configuration, Trunk port configuration. Users can configure trunk ports.

5.5.1.4.1 Vlan setting for trunk port

Click Vlan configuration, Vlan configuration, Trunk port configuration, Vlan setting for

trunk port. Users can configure vlan attributes of trunk ports:

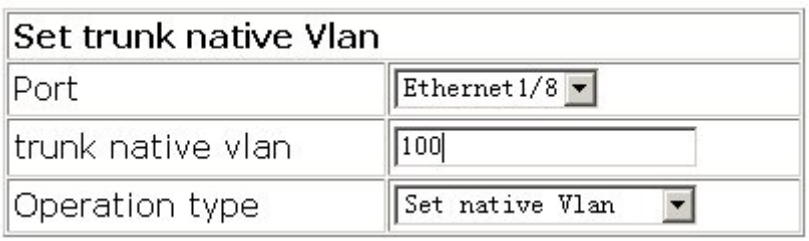
Set trunk native vlan: Set the native vlan of the port. See the equivalent CLI command at 5.2.2.7:

Port – Specify the port

Trunk native vlan – Specify native vlan id

Operation type – Set native vlan: Add new VLAN; Remove native vlan: Leave the native vlan

For example: Select port Ethernet1/8; set Trunk native vlan to 100; select Operation type to Set native vlan, and then click Set. The native vlan of Ethernet 1/8 is set to vlan 100.



Set trunk allow vlan: Set the allow vlan of the port. See the equivalent CLI command at 5.2.2.6:

Port – Specify the port

Trunk allow vlan list – Specify allow vlan id list

Operation type – Set allow vlan: Add new allow VLAN; Remove allow vlan: Remove allow vlan

For example: Select port Ethernet1/8; set Trunk allow vlan list to 31; set Operation type to Set allow vlan, and then click Set. The allow vlan of Ethernet 1/8 is set to vlan 31.



5.5.1.5 Allocate port for Vlan

Click Vlan configuration, Vlan configuration, Access port configuration. Users can configure VLAN of the Access port.

5.5.1.5.1 Vlan setting for access port

Click Vlan configuration, Vlan configuration, Access port configuration, Vlan setting

for access port. Users can add Access port to the specified VLAN, or delete Access port from the specified VLAN:

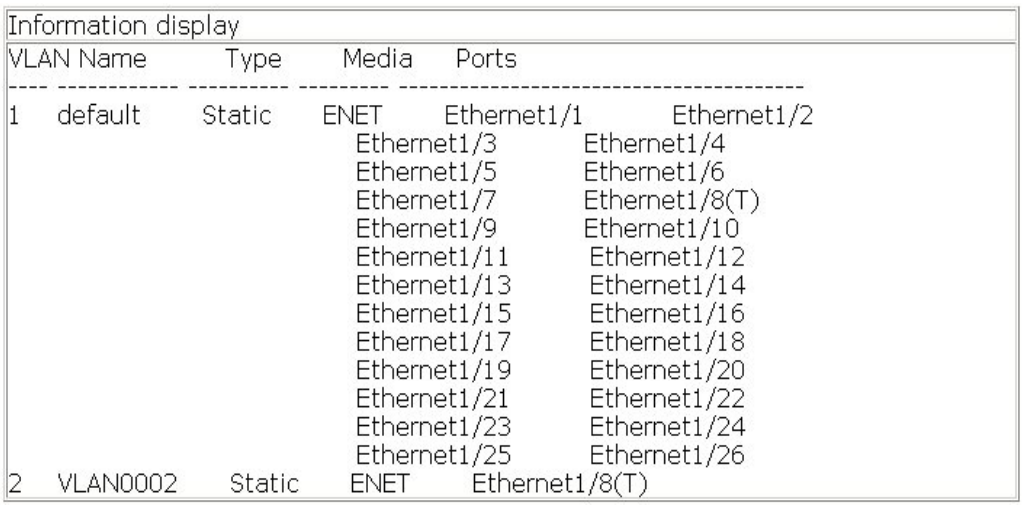
Port – Specify the port

Vlan ID – Specify VLAN ID

For example: Select port Ethernet1/1; select Vlan ID 1, and then click Apply. The port Ethernet 1/1 is added to VLAN 1.



The results are shown in Information Display window:



5.5.1.6 Allocate port for Vlan

Click Vlan configuration, Vlan configuration, Enable/Disable Vlan ingress rule. Users can configure VLAN ingress rules.

5.5.1.6.1 Disable Vlan ingress rules

Click Vlan configuration, Vlan configuration, Enable/Disable Vlan ingress rule, Disable Vlan ingress rules. Users can enable or disable VLAN ingress rules:

For example: Select port Ethernet1/1, and then click Apply. VLAN ingress rules on Ethernet 1/1 are disabled. Click Default, VLAN ingress rules on Ethernet 1/1 are enabled.



5.5.2 GVRP configuration

Click Vlan configuration, GVRP configuration. Users can configure GVRP.

5.5.2.1 Enable global GVRP

Click Vlan configuration, GVRP configuration, Enable global GVRP. Users can enable or disable GVRP globally. See the equivalent CLI command at 5.3.2.5.

For example: Select Enable GVRP, and then click Apply. The GVRP is enabled globally on the switch.



5.5.2.2 Enable port GVRP

Click Vlan configuration, GVRP configuration, Enable port GVRP. Users can enable or disable GVRP on the port. See the equivalent CLI command at 5.3.2.5

For example: Select port Ethernet1/1; select Enable GVRP, and then click Apply. The GVRP is enabled on Ethernet 1/1. Note: The GVRP can only be enabled on the trunk port.



5.5.2.3 GVRP configuration

Click Vlan configuration, GVRP configuration, GVRP configuration. Users can configure GVRP attributes on the switch:

Port – Specify the port

Join timer(100~327650ms) – Set GARP join timer. See the equivalent CLI command at 5.3.2.1

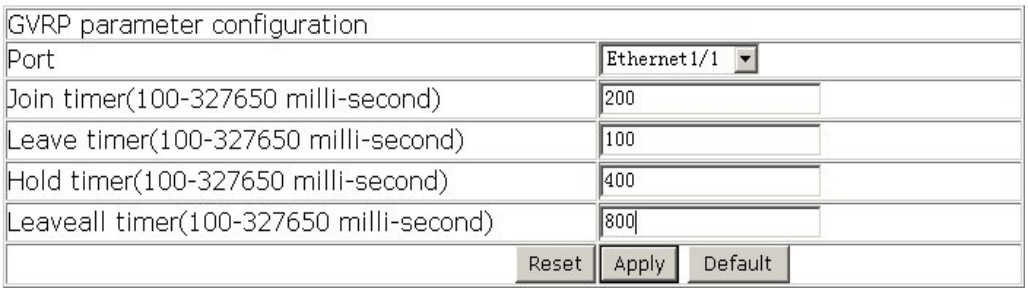
Leave timer(100~327650ms) – Set GARP leave timer. See the equivalent CLI command at 5.3.2.2

Hold timer(100~327650ms) – Set GARP hold timer. See the equivalent CLI command at 5.2.3.3

Leaveall timer(100~327650ms) – Set GARP leaveall timer. See the equivalent CLI command at 5.2.3.4

For example: Select port Ethernet1/1; set Join timer to 200; set Leave timer to 100; set Hold timer to 400; set Leaveall timer to 800, and then click Apply. The configuration is

applied on the switch.

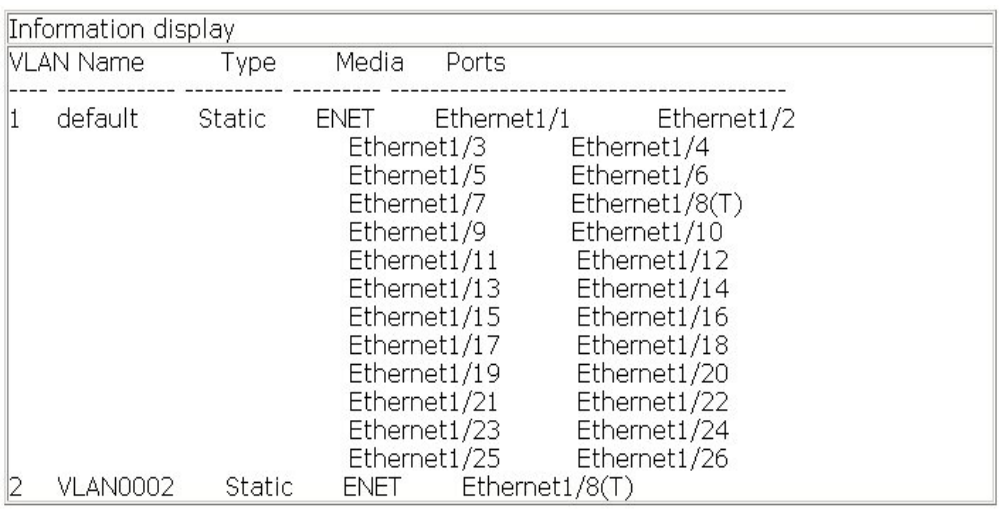


5.5.3 VLAN debug and maintenance

Click Vlan configuration, Vlan debug and maintenance. Users can view Vlan information on the switch.

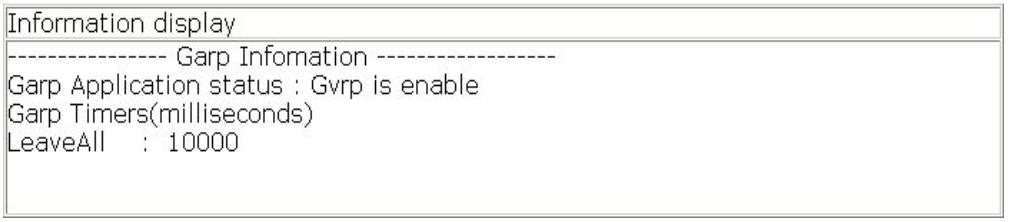
5.5.3.1 show Vlan

Click Vlan configuration, VLan debug and maintenance, show Vlan. The Vlan information is shown on Information display window. See the equivalent CLI command at 5.4.1.1



5.5.3.2 show garp

Click Vlan configuration, VLan debug and maintenance, show garp. The GARP information is shown on Information display window. See the equivalent CLI command at 5.4.1.2



5.5.3.3show gvrp

Click Vlan configuration, VLan debug and maintenance, show gvrp. The GVRP information is shown on Information display window. See the equivalent CLI command at 5.4.1.3



Chapter 6 MSTP Configuration

6.1 MSTP Introduction

The MSTP (Multiple STP) is a new spanning-tree protocol which is based on the STP and the RSTP. It runs on all the bridges of a bridged-LAN. It calculates a common and internal spanning tree (CIST) for the bridge-LAN which consists of the bridges running the MSTP, the RSTP and the STP. It also calculates the independent multiple spanning-tree instances (MSTI) for each MST domain (MSTP domain). The MSTP, which adopts the RSTP for its rapid convergence of the spanning tree, enables multiple VLANs to be mapped to the same spanning-tree instance which is independent to other spanning-tree instances. The MSTP provides multiple forwarding paths for data traffic and enables load balancing. Moreover, because multiple VLANs share a same MSTI, the MSTP can reduce the number of spanning-tree instances, which consumes less CPU resources and reduces the bandwidth consumption.

6.1.1MSTP Region

Because multiple VLANs can be mapped to a single spanning tree instance, IEEE 802.1s committee raises the MST concept. The MST is used to make the association of a certain VLAN to a certain spanning tree instance.

A MSTP region is composed of one or multiple bridges with the same MCID (MST Configuration Identification) and the bridged-LAN (a certain bridge in the MSTP region is the designated bridge of the LAN, and the bridges attaching to the LAN are not running STP). All the bridges in the same MSTP region have the same MSID.

MSID consists of 3 attributes:

- Configuration Name: Composed by digits and letters
- Revision Level
- Configuration Digest: VLANs mapping to spanning tree instances

The bridges with the same 3 above attributes are considered as in the same MST region.

When the MSTP calculates CIST in a bridged-LAN, a MSTP region is considered as a bridge. See the figure below:

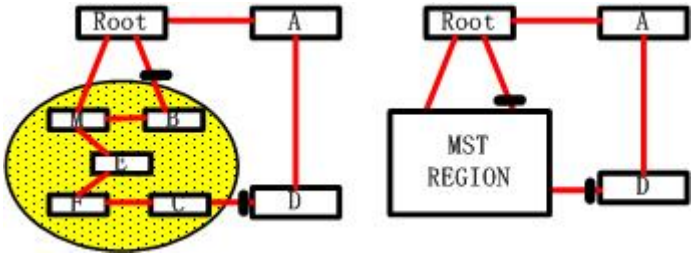


Figure 6-1 Example of CIST and MST Region

In the above network, if the bridges are running the STP other the RSTP, one port between Bridge M and Bridge B should be blocked. But if the bridges in the yellow range run the MSTP and are configured in the same MST region, MSTP will treat this region as a bridge. Therefore, one port between Bridge B and Root is blocked and one port on Bridge D is blocked.

6.1.1.1 Operations Within An MSTP Region

The IST connects all the MSTP bridges in a region. When the IST converges, the root of the IST becomes the IST master, which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master also is the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP bridges at the boundary of the region is sected as the IST master.

When an MSTP bridge initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The bridge also initializes all of its MST instances and claims to be the root for all of them. If the bridge receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

Within a MST region, the IST is the only spanning-tree instance that sends and receives BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth.

6.1.1.2 Operations between MST Regions

If there are multiple regions or legacy 802.1D bridges within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP bridges in the network. The MST instances combine with the IST at the boundary of the

region to become the CST.

The MSTI is only valid within its MST region. An MSTI has nothing to do with MSTIs in other MST regions. The bridges in a MST region receive the MST BPDU of other regions through Boundary Ports. They only process CIST related information and abandon MSTI information.

6.1.2 Port Roles

The MSTP bridge assigns a port role to each port which runs MSTP.

- CIST port roles: root port, designated port, alternate port and backup port
- On top of those roles, each MSTI port has one new role: master port.

The port roles in the CIST (root port, designated port, alternate port and backup port) are defined in the same ways as those in the RSTP.

6.1.3MSTP Load Balance

In a MSTP region, VLANs can by mapped to various instances. That can form various topologies. Each instance is independent from the others and each distance can has its own attributes such as bridge priority and port cost etc. Consequently, the VLANs in different instances have their own paths. The traffic of the VLANs are load-balanced.

6.2 Configuring MSTP

6.2.1 MSTP Configuration Task Sequence

1. Enable the MSTP and set the running mode
2. Configure instance parameters
3. Configure MSTP region parameters
4. Configure MSTP time parameters
5. Configure the fast migrate feature for MSTP

1. Enable MSTP and set the running mode

Command	Explanation
Global Mode and Interface Mode	

spanning-tree **no spanning-tree**	Enable/Disable MSTP
Global Mode	
spanning-tree mode {mstp|stp} **no spanning-tree mode**	Set MSTP running mode
Interface Mode	
spanning-tree mcheck	Force port migration to run under MSTP

2. Configure instance parameters

Command	**Explanation**
Global Mode	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	Set bridge priority for specified instance
Interface Mode	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	Set port path cost for specified instance
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*> port-priority**	Set port priority for specified instance

3. Configure MSTP region parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enter MSTP region mode. The " **no spanning-tree mst configuration**" command restores the default setting.
MSTP region mode	
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	Create Instance and set mapping between VLAN and Instance
name <*name*> **no name**	Set MSTP region name
revision-level <*level*> **no revision-level**	Set MSTP region revision level
abort	Quit MSTP region mode and return to Global mode without saving MSTP region configuration
exit	Quit MSTP region mode and return to Global mode with saving MSTP region configuration

4. Configure MSTP time parameters

Command	Explanation
Global Mode	
spanning-tree forward-time <*time*> **no spanning-tree forward-time**	Set the value for switch forward delay time
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	Set the Hello time for sending BPDU messages
spanning-tree maxage <*time*> **no spanning-tree maxage**	Set Aging time for BPDU messages
spanning-tree max-hop <*hop-count*> **no spanning-tree max-hop**	Set Maximum number of hops of BPDU messages in the MSTP region

5. Configure the fast migrate feature for MSTP

Command	Explanation
Interface Mode	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Set the port link type
spanning-tree portfast **no spanning-tree portfast**	Set the port to be an boundary port

6.2.2 MSTP Configuration Command

6.2.2.1 abort

Command: abort

Function: Abort the current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode: MSTP Region Mode

Usage Guide: This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid. This command is equal to "Ctrl+z".

Example: Quit MSTP region mode without saving the current configuration

Switch(Config-Mstp-Region)#abort

Switch(Config)#

6.2.2.2 exit

Command: exit

Function: Save current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode: MSTP Region Mode

Usage Guide: This command is to quit MSTP region mode with saving the current configuration.

Example: Quit MSTP region mode with saving the current configuration.

Switch(Config-Mstp-Region)#exit

Switch(Config)#

6.2.2.3 instance vlan

Command: instance <instance-id> vlan <vlan-list>

no instance <*instance-id*> [vlan <*vlan-list*>]

Function: In MSTP region mode, create the instance and set the mappings between VLANs and instances; The command "**no instance <*instance-id*> [vlan <*vlan-list*>]**" removes the specified instance and the specified mappings between the VLANs and instances.

Parameter: Normally, ***<instance-id>*** sets the instance number. The valid range is from 0 to 48.; In the command "**no instance <*instance-id*> [vlan <*vlan-list*>]**", ***<instance-id>*** sets the instance number. The valid number is from 1 to 48. ***<vlan-list>*** sets consecutive or non-consecutive VLAN numbers. "-" refers to consecutive numbers, and ";" refers to non-consecutive numbers.

Command mode: MSTP Region Mode

Default: Before creating any Instances, there is only the instance 0, and VLAN 1~5094 all belong to the instance 0.

Usage Guide: This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 48 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 48.

Example: Map VLAN1-10 and VLAN 100-110 to Instance 1.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

6.2.2.4 name

Command: name <*name*>

no name

Function: In MSTP region mode, set MSTP region name; The "**no name**" command restores the default setting.

Parameter: <*name*> is the MSTP region name. The length of the name should less than 32 characters.

Command mode: MSTP Region Mode

Default: Default MSTP region name is the MAC address of this bridge.

Usage Guide: This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.

Example: Set MSTP region name to mstp-test。

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#name mstp-test

6.2.2.5 revision-level

Command: revision-level <*level*>

no revision-level

Function: In MSTP region mode, this command is to set revision level for MSTP configuration; The command "**no revision-level**" restores the default setting to 0.

Parameter: <*level*> is revision level. The valid range is from 0 to 65535.

Command mode: MSTP Region Mode

Default: The default revision level is 0.

Usage Guide: This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.

Example: Set revision level to 2000。

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)# revision-level 2000

6.2.2.6 spanning-tree

Command: spanning-tree

no spanning-tree

Function: Enable MSTP in global mode and in interface mode; The command "**no spanning-tree**" is to disable MSTP.

Command mode: Global Mode and Interface Mode

Default: MSTP is not enabled by default.

Usage Guide: If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly.

Example: Enable the MSTP in global mode, and disable the MSTP in the interface 1/2.

Switch(Config)#spanning-tree

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#no spanning-tree

6.2.2.7 spanning-tree forward-time

Command: spanning-tree forward-time <*time*>

no spanning-tree forward-time

Function: Set the switch forward delay time; The command "**no spanning-tree forward-time**" restores the default setting.

Parameter: <*time*> is forward delay time in seconds. The valid range is from 4 to 30.

Command mode: Global Mode

Default: The forward delay time is 15 seconds by default.

Usage Guide: When the network topology changes, the status of the port is changed from

blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set MSTP forward delay time to 20 seconds.

Switch(Config)#spanning-tree forward-time 20

6.2.2.8 spanning-tree hello-time

Command: spanning-tree hello-time *<time>*

no spanning-tree hello-time

Function: Set switch Hello time; The command "**no spanning-tree hello-time**" restores the default setting.

Parameter: *<time>* is Hello time in seconds. The valid range is from 1 to 10.

Command mode: Global Mode

Default: Hello Time is 2 seconds by default.

Usage Guide: Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: Set MSTP hello time to 5 seconds in global mode.

Switch(Config)#spanning-tree hello-time 5

6.2.2.9 spanning-tree link-type p2p

Command: spanning-tree link-type p2p {auto|force-true|force-false}

no spanning-tree link-type

Function: Set the link type of the current port; The command "**no spanning-tree link-type**" restores link type to auto-negotiation.

Parameter: auto sets auto-negotiation, **force-true** forces the link as point-to-point type, **force-false** forces the link as non point-to-point type.

Command mode: Interface Mode

Default: The link type is auto by default, The MSTP detects the link type automatically.

Usage Guide: When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.

Example: Force the port 1/7-8 as point-to-point type.

Switch(Config)#interface ethernet 1/7-8

Switch(Config-Port-Range)#spanning-tree link-type p2p force-true

6.2.2.10 spanning-tree maxage

Command: spanning-tree maxage <*time*>

no spanning-tree maxage

Function: Set the max aging time for BPDU; The command "**no spanning-tree maxage**" restores the default setting.

Parameter: <*time*> is max aging time in seconds. The valid range is from 6 to 40.

Command mode: Global Mode

Default: The max age is 20 seconds by default.

Usage Guide: The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set max age time to 25 seconds.

Switch(Config)#spanning-tree maxage 25

6.2.2.11 spanning-tree max-hop

Command: spanning-tree max-hop <*hop-count*>

no spanning-tree max-hop

Function: Set maximum hops of BPDU in the MSTP region; The command "**no spanning-tree max-hop**" restores the default setting.

Parameter: <*hop-count*> sets maximum hops. The valid range is from 1 to 40.

Command mode: Global Mode

Default: The max hop is 20 by default.

Usage Guide: The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.

Example: Set max hop to 32.

Switch(Config)#spanning-tree max-hop 32

6.2.2.12 spanning-tree mcheck

Command: spanning-tree mcheck

Function: Force the port to run in the MSTP mode.

Command mode: Interface Mode

Default: The port is in the MSTP mode by default.

Usage Guide: If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.

This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.

Example: Force the port 1/2 to run in the MSTP mode.

Switch(Config-Ethernet1/2)#spanning-tree mcheck

6.2.2.13 spanning-tree mode

Command: spanning-tree mode {mstp|stp}

no spanning-tree mode

Function: Set the spanning-tree mode in the switch; The command "**no spanning-tree mode**" restores the default setting.

Parameter: mstp sets the switch in IEEE802.1s MSTP mode; **stp** sets the switch in IEEE802.1D STP mode.

Command mode: Global Mode

Default: The switch is in the MSTP mode by default.

Usage Guide: When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.

Example: Set the switch in the STP mode.

Switch(Config)#spanning-tree mode stp

6.2.2.14 spanning-tree mst configuration

Command: spanning-tree mst configuration

no spanning-tree mst configuration

Function: Enter the MSTP mode. Under the MSTP mode, the MSTP attributes can be set. The command "**no spanning-tree mst configuration**" restores the attributes of the MSTP to their default values.

Command mode: Global Mode

Default: The default values of the attributes of the MSTP region are listed as below:

Attribute of MSTP	Default Value
Instance	There is only the instance 0. All the VLANs (1~4094) are mapped to the instance 0.

Name	MAC address of the bridge
Revision	0

Usage Guide: Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.

Example: Enter MSTP region mode.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#

6.2.2.15 spanning-tree mst cost

Command: spanning-tree mst <*instance-id*> cost <*cost*>

no spanning-tree mst <instance-id> cost

Function: Sets path cost of the current port in the specified instance; The command "**no spanning-tree mst <instance-id> cost**" restores the default setting.

Parameter: <*instance-id*> sets the instance ID. The valid range is from 0 to 48. **<*cost*>** sets path cost. The valid range is from 1 to 200,000,000。

Command mode: Interface Mode

Default: By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Usage Guide: By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example: On the port 1/2, set the MSTP port cost in the instance 2 to 3000000.

Switch(Config-Ethernet1/2)#spanning-tree mst 2 cost 3000000

6.2.2.16 spanning-tree mst port-priority

Command: spanning-tree mst <*instance-id*> port-priority <*port-priority*>

no spanning-tree mst <*instance-id*> port-priority

Function: Set the current port priority for the specified instance; The command "**no spanning-tree mst <*instance-id*> port-priority**" restores the default setting.

Parameter: <*instance-id*> sets the instance ID. The valid range is from 0 to 48; **<*port-priority*>** sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32…240.

Command mode: Interface Mode

Default: The default port priority is 128.

Usage Guide: By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Example: Set the port priority as 32 on the port 1/2 for the instance 1.

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#spanning-tree mst 1 port-priority 32

6.2.2.17 spanning-tree mst priority

Command: spanning-tree mst <*instance-id*> priority <*bridge-priority*>

no spanning-tree mst <*instance-id*> priority

Function: Set the bridge priority for the specified instance; The command "**no spanning-tree mst <*instance-id*> priority**" restores the default setting.

Parameter: <*instance-id*> sets instance ID. The valid range is from 0 to 48; **<*bridge-priority*>** sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192…61440.

Command mode: Global Mode

Default: The default bridge priority is 32768。

Usage Guide: By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.

Example: Set the priority for Instance 2 to 4096.

Switch(Config)#spanning-tree mst 2 priority 4096

6.2.2.18 spanning-tree portfast

Command: spanning-tree portfast

no spanning-tree portfast

Function: Set the current port as boundary port; The command "**no spanning-tree portfast**" sets the current port as non-boundary port.

Command mode: Interface Mode

Default: All the ports are non-boundary ports by default when enabling MSTP.

Usage Guide: When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.

Example: Set port 1/5-6 as boundary ports.

Switch(Config)#interface ethernet 1/5-6

Switch(Config-Port-Range)#spanning-tree portfast

6.3 MSTP Example

The following is a typical MSTP application scenario:

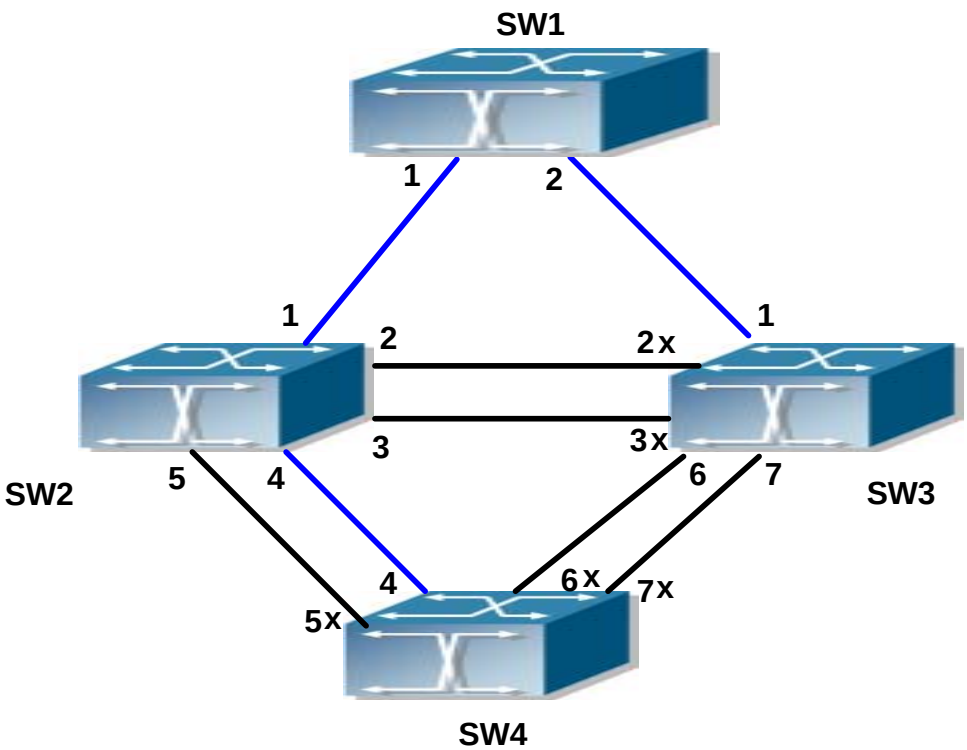


Figure 6-2 Typical MSTP Application Scenario

The connections among the switches are shown in the above figure. All the switches run in the MSTP mode by default, their bridge priority, port priority and port route cost are all in the default values (equal). The default configuration for switches is listed below:

Bridge Name	SW1	SW2	SW3	SW4
Bridge MAC	…00-00-01	…00-00-02	…00-00-03	…00-00-04

Address					
Bridge Priority		32768	32768	32768	32768
Port Priority	Port 1	128	128	128	
	Port 2	128	128	128	
	Port 3		128	128	
	Port 4		128		128
	Port 5		128		128
	Port 6			128	128
	Port 7			128	128
Route Cost	Port 1	200000	200000	200000	
	Port 2	200000	200000	200000	
	Port 3		200000	200000	
	Port 4		200000		200000
	Port 5		200000		200000
	Port 6			200000	200000
	Port 7			200000	200000

By default, the MSTP establishes a tree topology (in blue lines) rooted with SW1. The ports marked with “x” are in the discarding status, and the other ports are in the forwarding status.

Configurations Steps:

Step 1: Configure port to VLAN mapping:

- Create VLAN 20, 30, 40, 50 in SW2, SW3 and SW4.
- Set ports 1-7 as trunk ports in SW2, SW3 and SW4.

Step 2: Set SW2, SW3 and SW4 in the same MSTP:

- Set SW2, SW3 and SW4 to have the same region name as mstp.
- Map VLAN 20 and VLAN 30 in SW2, SW3 and SW4 to Instance 3; Map VLAN 40 and VLAN 50 in SW2, SW3 and SW4 to Instance 4.

Step 3: Set SW3 as the root bridge of Instance 3; Set SW4 as the root bridge of Instance 4

- Set the bridge priority of Instance 3 in SW3 as 0.
- Set the bridge priority of Instance 4 in SW4 as 0.

The detailed configuration is listed below:

SW2:

SW2(Config)#vlan 20

SW2(Config-Vlan20)#exit

```
SW2(Config)#vlan 30
SW2(Config-Vlan30)#exit
SW2(Config)#vlan 40
SW2(Config-Vlan40)#exit
SW2(Config)#vlan 50
SW2(Config-Vlan50)#exit
SW2(Config)#spanning-tree mst configuration
SW2(Config-Mstp-Region)#name mstp
SW2(Config-Mstp-Region)#instance 3 vlan 20;30
SW2(Config-Mstp-Region)#instance 4 vlan 40;50
SW2(Config-Mstp-Region)#exit
SW2(Config)#interface e1/1-7
SW2(Config-Port-Range)#switchport mode trunk
SW2(Config-Port-Range)#exit
SW2(Config)#spanning-tree
```

SW3:

```
SW3(Config)#vlan 20
SW3(Config-Vlan20)#exit
SW3(Config)#vlan 30
SW3(Config-Vlan30)#exit
SW3(Config)#vlan 40
SW3(Config-Vlan40)#exit
SW3(Config)#vlan 50
SW3(Config-Vlan50)#exit
SW3(Config)#spanning-tree mst configuration
SW3(Config-Mstp-Region)#name mstp
SW3(Config-Mstp-Region)#instance 3 vlan 20;30
SW3(Config-Mstp-Region)#instance 4 vlan 40;50
SW3(Config-Mstp-Region)#exit
SW3(Config)#interface e1/1-7
SW3(Config-Port-Range)#switchport mode trunk
SW3(Config-Port-Range)#exit
SW3(Config)#spanning-tree
SW3(Config)#spanning-tree mst 3 priority 0
```

SW4:

```
SW4(Config)#vlan 20
```

```
SW4(Config-Vlan20)#exit
SW4(Config)#vlan 30
SW4(Config-Vlan30)#exit
SW4(Config)#vlan 40
SW4(Config-Vlan40)#exit
SW4(Config)#vlan 50
SW4(Config-Vlan50)#exit
SW4(Config)#spanning-tree mst configuration
SW4(Config-Mstp-Region)#name mstp
SW4(Config-Mstp-Region)#instance 3 vlan 20;30
SW4(Config-Mstp-Region)#instance 4 vlan 40;50
SW4(Config-Mstp-Region)#exit
SW4(Config)#interface e1/1-7
SW4(Config-Port-Range)#switchport mode trunk
SW4(Config-Port-Range)#exit
SW4(Config)#spanning-tree
SW4(Config)#spanning-tree mst 4 priority 0
```

After the above configuration, SW1 is the root bridge of the instance 0 of the entire network. In the MSTP region which SW2, SW3 and SW4 belong to, SW2 is the region root of the instance 0, SW3 is the region root of the instance 3 and SW4 is the region root of the instance 4. The traffic of VLAN 20 and VLAN 30 is sent through the topology of the instance 3. The traffic of VLAN 40 and VLAN 50 is sent through the topology of the instance 4. And the traffic of other VLANs is sent through the topology of the instance 0. The port 1 in SW2 is the master port of the instance 3 and the instance 4.

The MSTP calculation generates 3 topologies: the instance 0, the instance 3 and the instance 4 (marked with blue lines). The ports with the mark “x” are in the status of discarding. The other ports are the status of forwarding. Because the instance 3 and the instance 4 are only valid in the MSTP region, the following figure only shows the topology of the MSTP region.

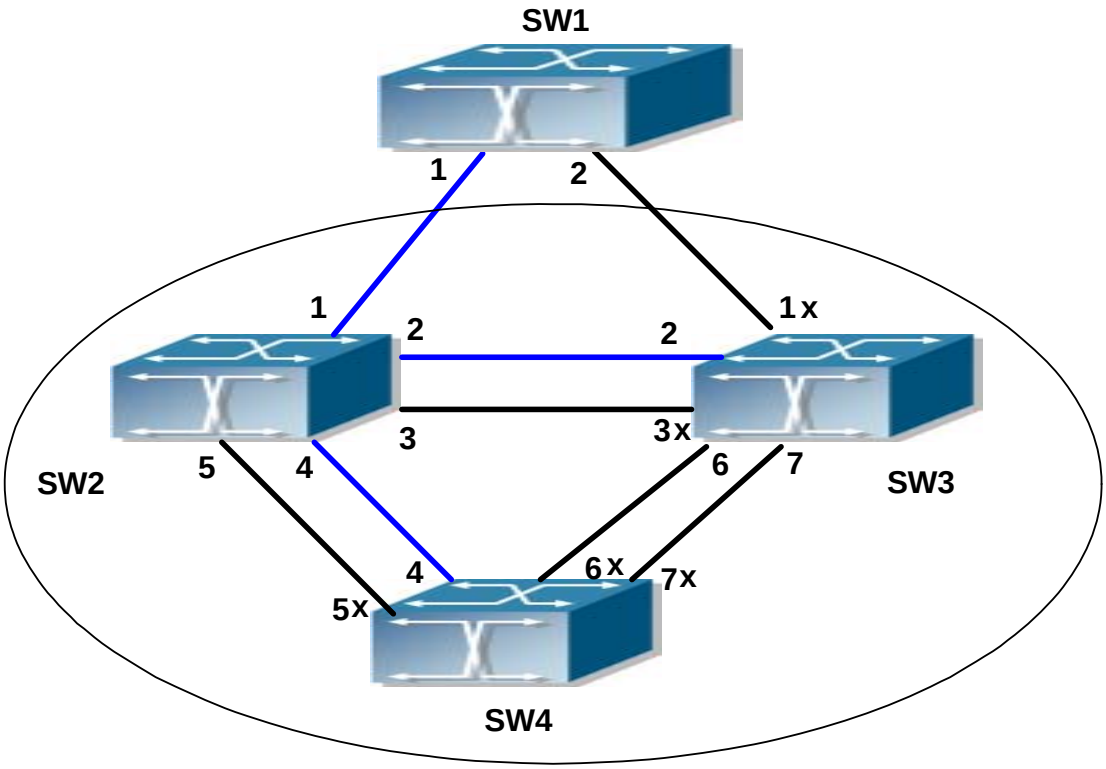


Figure 6-3 The Topology Of the Instance 0 after the MSTP Calculation

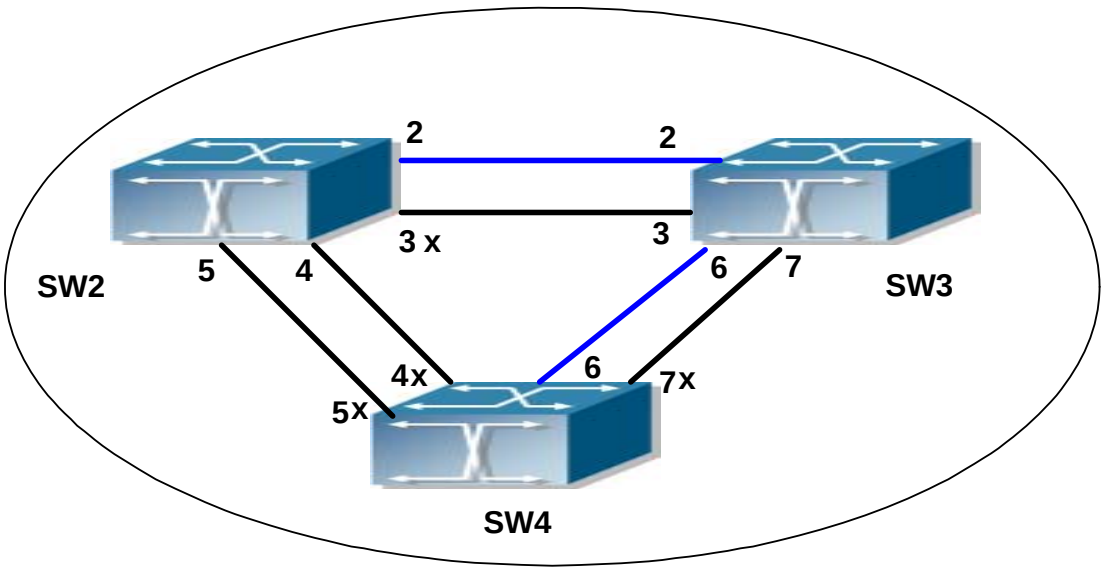


Figure 6-4 The Topology Of the Instance 3 after the MSTP Calculation

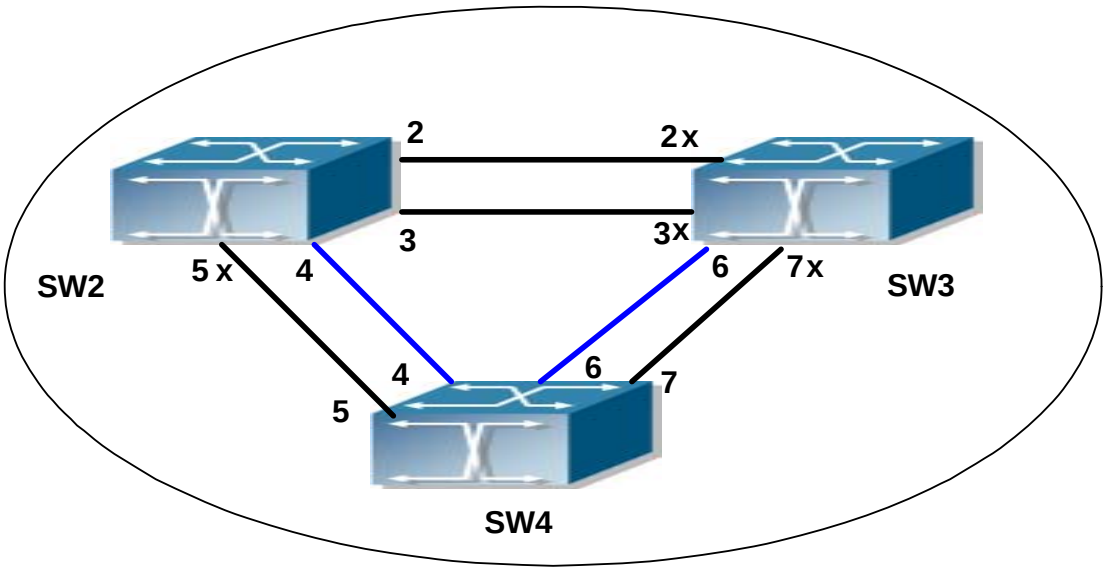


Figure 6-5 The Topology Of the Instance 4 after the MSTP Calculation MSTP Troubleshooting

6.4 MSTP Troubleshooting

6.4.1Monitoring And Debugging Command

6.4.1.1 show spanning-tree

Command: show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]

Function: Display the MSTP Information.

Parameter: **<*instance-id*>** sets the instance ID. The valid range is from 0 to 48; **<*interface-list*>** sets interface list; **detail** sets the detailed spanning-tree information.

Command mode: Privileged Mode

Usage Guide: This command can display the MSTP information of the instances in the current bridge.

Example: Display the bridge MSTP.

Switch#sh spanning-tree

-- MSTP Bridge Config Info --

Standard : IEEE 802.1s

Bridge MAC : 00: 03: 0f: 01: 0e: 30

Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15

Force Version: 3

############################ Instance 0 ############################
Self Bridge Id : 32768 - 00: 03: 0f: 01: 0e: 30
Root Id : 16384.00: 03: 0f: 01: 0f: 52
Ext.RootPathCost : 200000
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 128.1
Current port list in Instance 0:
Ethernet1/1 Ethernet1/2 (Total 2)

PortName	ID	ExtRPC	IntRPC	State	Role	DsgBridge	DsgPort
Ethernet1/1	128.001	0	0	FWD	ROOT	16384.00030f010f52	128.007
Ethernet1/2	128.002	0	0	BLK	ALTR	16384.00030f010f52	128.011

############################ Instance 3 ############################
Self Bridge Id : 0.00: 03: 0f: 01: 0e: 30
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 3:
Ethernet1/1 Ethernet1/2 (Total 2)

PortName	ID	IntRPC	State	Role	DsgBridge	DsgPort
Ethernet1/1	128.001	0	FWD	MSTR	0.00030f010e30	128.001
Ethernet1/2	128.002	0	BLK	ALTR	0.00030f010e30	128.002

############################ Instance 4 ############################
Self Bridge Id : 32768.00: 03: 0f: 01: 0e: 30
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 4:
Ethernet1/1 Ethernet1/2 (Total 2)

```
  PortName        ID      IntRPC    State Role       DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1 128.001             0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet1/2 128.002             0 BLK ALTR 32768.00030f010e30 128.002
```

Displayed Information	Description
Bridge Information	
Standard	STP version
Bridge MAC	Bridge MAC address
Bridge Times	Max Age, Hello Time and Forward Delay of the bridge
Force Version	Version of STP
Instance Information	
Self Bridge Id	The priority and the MAC address of the current bridge for the current instance
Root Id	The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the region root of the current instance
Root Port ID	Root port of the current instance on the current bridge
MSTP Port List Of The Current Instance	
PortName	Port name
ID	Port priority and port index
ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the region root of the current instance
State	Port status of the current instance
Role	Port role of the current instance
DsgBridge	Upward designated bridge of the current port in the current instance
DsgPort	Upward designated port of the current port in the current instance

6.4.1.2 show mst configuration

Command: show spanning-tree mst config

Function: Display the configuration of the MSTP in the privileged mode.

Command mode: Privileged Mode

Usage Guide: In the privileged mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

Example: Display the configuration of the MSTP on the switch.

Switch#show spanning-tree mst config

Name switch
Revision 0
Instance Vlans Mapped
---
00 1-29, 31-39, 41-4094
03 30
04 40

6.4.1.3 show mst-pending

Command: show mst-pending

Function: In the MSTP region mode, display the configuration of the current MSTP region.

Command mode: MSTP Region Mode

Usage Guide: In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.

Note: Before quitting the MSTP region mode, the displayed parameters may not be effective.

Example: Display the configuration of the current MSTP region.

Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending

Name switch
Revision 0
Instance Vlans Mapped
---
00 1-29, 31-39, 41-4093
03 30
04 40
05 4094

Switch(Config-Mstp-Region)#

6.4.1.4debug spanning-tree

Command: debug spanning-tree

no debug spanning-tree

Function: Enable the MSTP debugging information; The command "**no debug spanning-tree**" disables the MSTP debugging information

Command mode: Privileged Mode

Usage Guide: This command is the general switch for all the MSTP debugging. Users should enable the detailed debugging information, then they can use this command to display the relevant debugging information. In general, this command is used by skilled technicians.

Example: Enable to receive the debugging information of BPDU messages on the port 1/1

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/1

6.4.2 MSTP Troubleshooting Help

- ☞ In order to run the MSTP on the switch port, the MSTP has to be enabled globally. If the MSTP is not enabled globally, it can't be enabled on the port.
- ☞ The MSTP parameters co work with each other, so the parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

  2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- ☞ When users modify the MSTP parameters, they have to be sure about the changes of the topologies. The global configuration is based on the bridge. Other configurations are based on the individual instances.
- ☞ The MSTP are mutually exclusive with MAC binding and IEEE 802.1x on the switch port. If MAC binding or IEEE 802.1x is enabled on the port, the MSTP can't apply to this port.

Chapter 7 IGMP Snooping Configuration

7.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network devices (such as routers) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send an IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with an IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and decides multicast packet forwarding according to the forwarding table.

ES4626/ES4650 provides IGMP Snooping and is able to send a query from the switch so that the user can use ES4626/ES4650 in IP multicast.

7.2 IGMP Snooping Configuration

7.2.1 IGMP Snooping Configuration Task

1. Enable IGMP Snooping
2. Configure IGMP Snooping
3. Configure sending of IGMP Query

1. Enable IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping **no ip igmp snooping**	Enable IGMP Snooping

2. Configure IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enable IGMP Snooping for specified VLAN
ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> mrouter**	Set in the specified VLAN the port for connecting M-router
ip igmp snooping vlan <*vlan-id*> immediate-leave **no ip igmp snooping vlan <*vlan-id*> immediate-leave**	Enable IGMP Snooping in the specified VLAN to quickly leave multicast group
ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*> interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*>**	Configure static multicast address and port member to join

3. Configure IGMP to send Query

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> query **no ip igmp snooping vlan <*vlan-id*> query**	Enable IGMP Snooping of specified VLAN to send a query
ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*> **no ip igmp snooping vlan <*vlan-id*> query robustness**	Set the robustness parameter for IGMP Snooping Query of specified VLAN
ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*> **no ip igmp snooping vlan <*vlan-id*> query interval**	Set the query interval for IGMP Snooping Query of specified VLAN
ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*> **no ip igmp snooping vlan <*vlan-id*>**	Set the maximum response time for IGMP Snooping Query of specified VLAN

query max-response-time	

7.2.2 IGMP Snooping Configuration Command

7.2.2.1 ip igmp snooping

Command: ip igmp snooping
no ip igmp snooping

Function: Enable the IGMP Snooping function in the switch: the "**no ip igmp snooping**" command disables the IGMP Snooping function.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: Enabling IGMP Snooping to allow the switch to monitor multicast traffic in the network and decide which ports can receive multicast traffic.

Example: Enable IGMP Snooping in Global Mode.

Switch(Config)#ip igmp snooping

7.2.2.2 ip igmp snooping vlan

Command: ip igmp snooping vlan <*vlan-id*>
no ip igmp snooping vlan <*vlan-id*>

Function: Enable the IGMP Snooping function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameter: <*vlan-id*> is the VLAN number.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: IGMP Snooping for the switch must be enabled first to enable IGMP Snooping for the specified VLAN. This command cannot be used with **ip igmp snooping vlan <*vlan-id*> query** command, i.e. either snooping or query can be enabled for one VLAN, but not both.

Example: Enable IGMP Snooping for VLAN 100 in Global Mode.

Switch(Config)#ip igmp snooping vlan 100

7.2.2.3 ip igmp snooping vlan mrouter

Command: ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*>
no ip igmp snooping vlan <*vlan-id*> mrouter

Function: Specify static multicast router port in the VLAN; the "**no ip igmp snooping vlan <*vlan-id*> mrouter**" command deletes multicast router port.

Parameter: **<*vlan-id*>** is the specified VLAN number; ***<interface –name>*** is the specified multicast router port number.

Command mode: Global Mode

Default: No M-Router port is set in the default VLAN.

Usage Guide: M-Router port must be set in a VLAN enabled IGMP Snooping, or the IGMP packet will be discarded so that IGMP Snooping cannot be performed in the specified VLAN.

Example: Set port 1/6 of VLAN 100 to be the M-Router port.

Switch(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/6

7.2.2.4 ip igmp snooping vlan static

Command: ip igmp snooping vlan <*vlan-id*> static <multicast-ip-addr> interface <*interface –name*>

no ip igmp snooping vlan <*vlan-id*> static <multicast-ip-addr>

Function: Enable the IGMP Snooping static multicast group membership: the "**no ip igmp snooping vlan <vlan-id> static <multicast-ip-addr>**" command disables the function.

Parameter: **<*mac-id*>** stands for the specified VLAN number; ***<multicast-ip-addr>*** for multicast MAC address; ***<interface-name>*** for multicast group member port. .

Command mode: Global Mode

Default: No static multicast group is set by default.

Usage Guide: If the static multicast address to be added exists and is a dynamic address, the static address overwrites the dynamic one.

Example: Create a new static multicast address 224.1.1.1 in VLAN 100 and include port 1/6 in the group.

Switch(Config)#ip igmp snooping vlan 100 static 224.1.1.1 interface ethernet 1/6

Delete static multicast address 224.1.1.1 in VLAN 100.

Switch(Config)#no ip igmp snooping vlan 100 static 224.1.1.1

7.2.2.5 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan <*vlan-id*> immediate-leave

no ip igmp snooping vlan <*vlan-id*> immediate-leave

Function: Enable the IGMP fast leave function for the specified VLAN: the "**no ip igmp**

snooping vlan <vlan-id> immediate-leave" command disables the IGMP fast leave function.

Parameter: <*vlan-id*> is the VLAN number specified.

Command mode: Global Mode

Default: This function is disabled by default.

Usage Guide: Enabling IGMP fast leave function speeds up the process for port to leave multicast group. This command is valid only in Snooping, and is not applicable to Query.

Example: Enable the IGMP fast leave function for VLAN 100.

Switch(Config)#ip igmp snooping vlan 100 immediate-leave

7.2.2.6 ip igmp snooping vlan query

Command: ip igmp snooping vlan <*vlan-id*> query

no ip igmp snooping vlan <*vlan-id*> query

Function: Enable the IGMP Query function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query**" command disables the Query function.

Parameter: <*vlan-id*> is the VALN number specified.

Command mode: Global Mode

Default: IGMP Query is disabled by default.

Usage Guide: Before enabling the IGMP Query function for the specified VLAN, the switch must have a corresponding VLAN configured and IGMP Snooping enabled. It should be noted that this command cannot be used with **ip igmp snooping vlan <*vlan-id*>** command, i.e. either snooping or query can be enabled for one VLAN, but not both.

Example: Enable the IGMP Query function for VLAN 100.

Switch(Config)#ip igmp snooping vlan 100 query

7.2.2.7 ip igmp snooping vlan query robustness

Command: ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*>

no ip igmp snooping vlan <*vlan-id*> query robustness

Function: Enable the IGMP Query function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query robustness**" command restores the default setting.

Parameter: <*vlan-id*> is the specified VLAN number; **<*robustness-variable*>** is robustness parameter, the valid range is 2 to 10.

Command mode: Global Mode

Default: The default robustness parameter is 2.

Usage Guide: Larger robustness; parameter means worse network conditions; smaller robustness; parameter means better network conditions. The user can set the robustness parameter according to their network conditions.

Example: Set the robustness parameter for the IGMP Query of VLAN 100 to 3.

Switch(Config)#ip igmp snooping vlan 100 query robustness 3

7.2.2.8 ip igmp snooping vlan query interval

Command: ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*>
no ip igmp snooping vlan <*vlan-id*> query interval

Function: Set the IGMP Query interval for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query interval**" command restores the default setting.

Parameter: <*vlan-id*> is the specified VLAN number; **<*interval-value*>** is the query interval, valid range is 1 to 65535.

Command mode: Global Mode

Default: The default interval is 125 seconds.

Example: Set the IGMP Query interval for VLAN 100 to 60 seconds.

Switch(Config)#ip igmp snooping vlan 100 query interval 60

7.2.2.9 ip igmp snooping vlan query max-response-time

Command: ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*>
no ip igmp snooping vlan <*vlan-id*> query max-response-time

Function: Set the maximum IGMP Query response time for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query max-response-time**" command restores the default setting.

Parameter: <*vlan-id*> is the specified VLAN number; **<*time-value*>** is maximum query response time, valid range is 10 to 25.

Command mode: Global Mode

Default: The maximum response time is 10 seconds.

Example: Set the maximum IGMP Query response time of VLAN 100 to 12 seconds.

Switch(Config)#ip igmp snooping vlan 100 query max-response-time 12

7.3 IGMP Snooping Example

Scenario 1. IGMP Snooping function

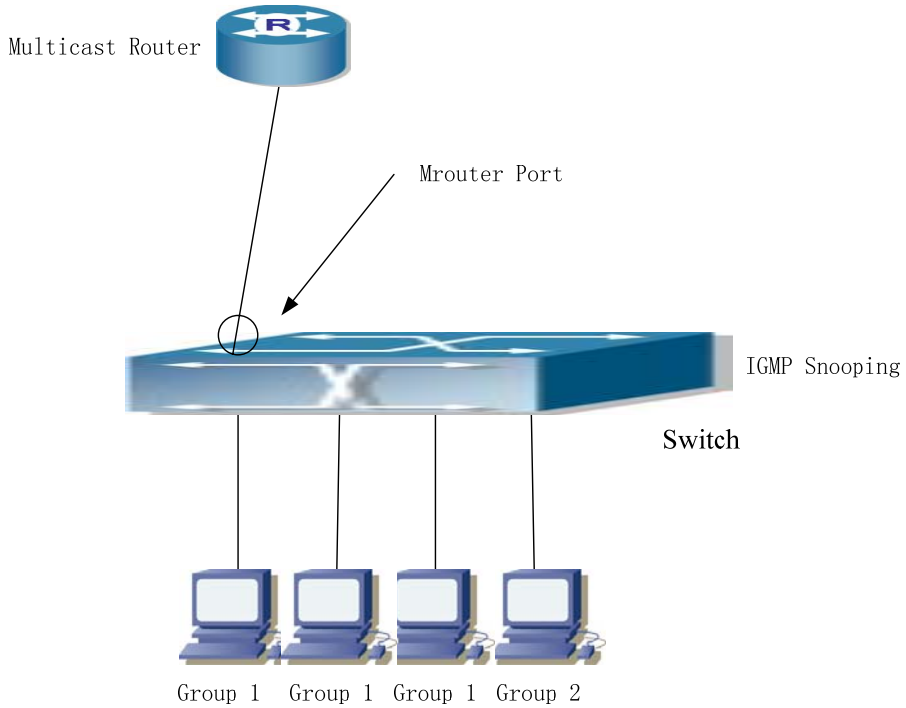


Fig 7-1 Enabling IGMP Snooping function

As shown in the above figure, a VLAN 100 is configured in the switch, including port 1, 2, 6, 10 and 12 on slot 1. Four hosts are connected to port 2, 6, 10, 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, if IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100, and port 1 of VLAN 100 to be the M-Router port.

The configuration steps are listed below:

Switch#config

Switch(Config)#ip igmp snooping

Switch(Config)#ip igmp snooping vlan 100

Switch(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host connected to port 12 plays program 2.

IGMP Snooping listening result:

The multicast table built by IGMP Snooping in VLAN 100 indicates port 1, 2, 6, 10 in Group1 and port 1, 12 in Group2.

All the four hosts can receive the program of their choice: port 2, 6, 10 will not receive

traffic of program 2 and port 12 will not receive traffic of program 1.

Scenario2IGMPQuery

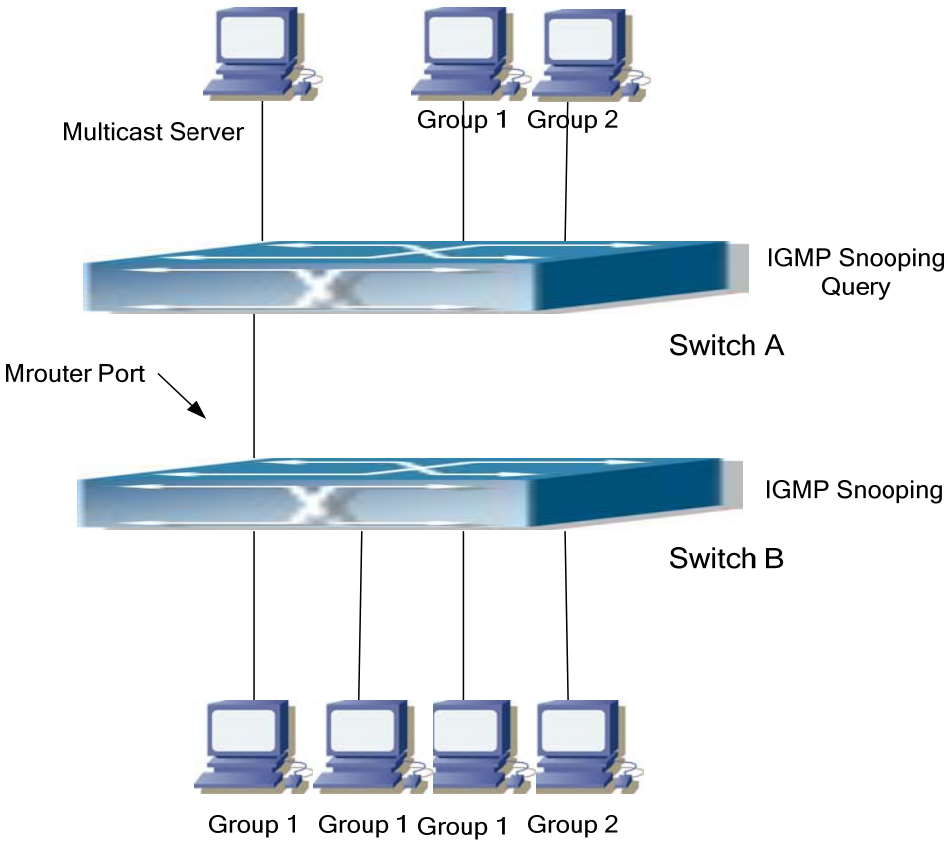


Fig 7-2 The switches as IGMP Queriers

The configuration of Switch2 is the same as the switch in scenario 1, Switch1 takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in Switch1, including port 1, 2, 6, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enable in Global mode and in VLAN60.

The configuration steps are listed below:

Switch1#config

Switch1(Config)#ip igmp snooping

Switch1(Config)#ip igmp snooping vlan 60 query

Switch2#config

Switch2(Config)#ip igmp snooping

Switch2(Config)#ip igmp snooping vlan 100

Switch2(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

The same as scenario 1.

IGMP Snooping listening result:

Similar to scenario 1.

7.4 IGMP Snooping Troubleshooting Help

7.4.1 Monitor and Debug Commands

7.4.1.1 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]

Parameter: ***<vlan-id>*** is id of VLAN to display the IGMP Snooping information.

Command mode: Admin Mode

Usage Guide: If VLAN id is not specified, then summary information for IGMP Snooping and Query in all VLAN will be displayed. If VLAN id is specified, then detailed information for IGMP Snooping and Query of the specified VLAN will be displayed.

Example:

1. Display the summery information of IGMP Snooping and Query for the switch.

```
Switch#show ip igmp snooping
igmp snooping status                : Enabled
IGMP information for VLAN 1:

igmp snooping vlan status           : Disabled
igmp snooping vlan query            : Disabled
igmp snooping vlan mrouter port : (null)--------------------------------

IGMP information for VLAN 2:

igmp snooping vlan status           : Enabled
igmp snooping vlan query            : Disabled
igmp snooping vlan mrouter port : (null)
------------------------------

IGMP information for VLAN 3:
```

igmp snooping vlan status : Disabled
igmp snooping vlan query : Disabled
igmp snooping vlan mrouter port : (null)

IGMP information for VLAN 4:
igmp snooping vlan status : Disabled
igmp snooping vlan query : Disabled
igmp snooping vlan mrouter port : (null)

IGMP information for VLAN 511:

igmp snooping vlan status : Disabled
igmp snooping vlan query : Disabled
igmp snooping vlan mrouter port : (null)

IGMP information for VLAN 5:

igmp snooping vlan status : Disabled
igmp snooping vlan query : Disabled
igmp snooping vlan mrouter port : (null)

Displayed information	Explanation
igmp snooping status	whether “igmp snooping” function is enabled.
igmp snooping vlan status	“igmp snooping” status of all VLANs in the switch(enabled or not).
igmp snooping vlan query	Query status of all VLANs in the switch(enabled or not).
igmp snooping vlan mrouter port	All M-Router port number (if any) of all VLANs in the switch
igmp snooping vlan mrouter state	All M-Router port (if any) status of all VLANs in the switch, this will not be displayed if no M-Router port is specified.

2. Display detailed information of IGMP Snooping and Query for VLAN2.
Switch#show ip igmp snooping vlan 2
IGMP information for VLAN 2:

```
igmp snooping status                          : Enabled
igmp snooping vlan status                     : Enabled
igmp snooping vlan mrouter port                    : Ethernet1/4
igmp snooping vlan mrouter state                   : UP
igmp snooping vlan mrouter present            : Yes
igmp snooping vlan immediate leave                 : No
igmp snooping vlan query                      : Disabled
igmp snooping vlan robustness                 : 2
igmp snooping vlan query interval                  : 125
igmp snooping vlan query max response time    : 10
igmp snooping vlan query TX                   : 0
igmp snooping vlan query SX                        : 2
igmp snooping multicast information:
MAC address                          Member port list
-------------------------------------------------------------
01-00-5E-7F-28-B3                    Ethernet1/5
-------------------------------------------------------------
01-00-5E-7F-30-BD              Ethernet1/4    Ethernet1/5
```

Sort by port:

```
Port              State                Type                  Group Address        Life
-------------------------------------------------------------------------------
Ethernet1/4       MEMBERS_PRESENT      Snoop_Group_Addr      239.255.48.189
0
-------------------------------------------------------------------------------
Ethernet1/5       MEMBERS_PRESENT      Snoop_Group_Addr      239.255.40.179
0
                  MEMBERS_PRESENT      Snoop_Group_Addr      239.255.48.189
0
-------------------------------------------------------------------------------
```

Displayed information	Explanation
igmp snooping status	whether “igmp snooping” function is enabled.
igmp snooping vlan status	“igmp snooping” status of the VLAN (enabled or not).
igmp snooping vlan query	“igmp query” status of the VLAN (enabled or not).
igmp snooping vlan mrouter	M-Router port number (if any) of the VLAN

port	
igmp snooping vlan mrouter state	All M-Router port (if any) status of all VLANs in the switch, this will not be displayed if no M-Router port is specified.
igmp snooping vlan mrouter present	Whether query packets present in the M-Router
igmp snooping vlan query TX	Query packet number sent by the VLAN
igmp snooping vlan query SX	Query packet number received by the VLAN
igmp snooping multicast mac	Multicast addresses learnt by the IGMP Snooping forward table.
igmp snooping multicast port	The member port name corresponding to each multicast MAC address in the IGMP Snooping forward table.

7.4.1.2 show mac-address-table multicast

Command: show mac-address-table multicast [vlan <*vlan-id*>]

Function: Display information for the multicast MAC address table.

Parameter: <*vlan-id*> is the VLAN ID to be included in the display result.

Command mode: Admin Mode

Default: Multicast MAC address-port mapping is not displayed by default.

Usage Guide: This command can be used to display the multicast6 MAC address table for the current switch.

Example: Display the multicast mapping for VLAN100.

```
Switch#show mac-address-table multicast vlan 100
Vlan Mac Address                    Type      Ports
---- --------------------------- ------- -----------------------------------
100   01-00-5e-01-01-01             MULTI     IGMP        Ethernet1/2
```

7.4.1.3 debug igmp snooping

Command: debug ip igmp snooping

no debug ip igmp snooping

Function: Enable the IGMP Snooping debug function: the " **no debug ip igmp snooping"** command disables this debug function**.**

Command mode: Admin Mode

Default: IGMP Snooping debug is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping debug, IGMP packet

processing information can be displayed.

Example: Enable IGMP Snooping debug.

Switch#debug ip igmp snooping

7.4.2 IGMP Snooping Troubleshooting Help

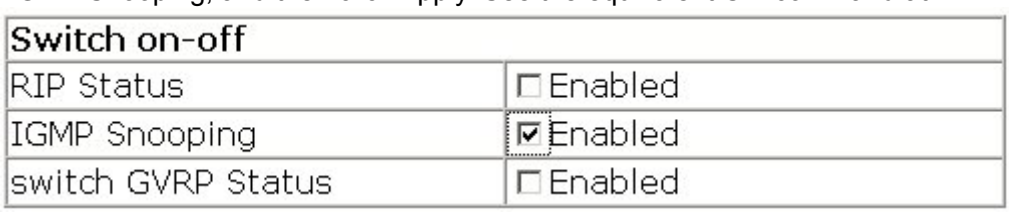
- ☞ IGMP Snooping function cannot be used with IGMP Query, Snooping is not available when Query is enabled. The user must make sure whether IGMP Snooping or IGMP Query is to be enabled.
- ☞ When IGMP Snooping is used, M-Router port must be specified in the corresponding VLAN, or the switch cannot perform IGMP Snooping properly.

7.5 Web Management

Click IGMP Snooping configuration. IGMP Snooping configuration and IGMP Snooping static multicast configuration are shown. On IGMP Snooping configuration page, users can configure IGMP snooping and query; on IGMP Snooping static multicast configuration page, users can configure static multicast and IGMP snooping.

7.5.1Enable IGMP Snooping on the switch

Click Switch basic configuration, Switch on-off configuration. Check “Enabled” box after IGMP Snooping, and then click Apply. See the equivalent CLI command at 7.2.2.1



7.5.2 IGMP Snooping Configuration

Click IGMP Snooping configuration. The IGMP Snooping configuration page is shown. The configuration page consists of 3 parts: query configuration, snooping configuration and IGMP configuration.

7.5.2.1Query configuration

The explanation of each field is as below:

VLAN ID – Configure query vlan ID

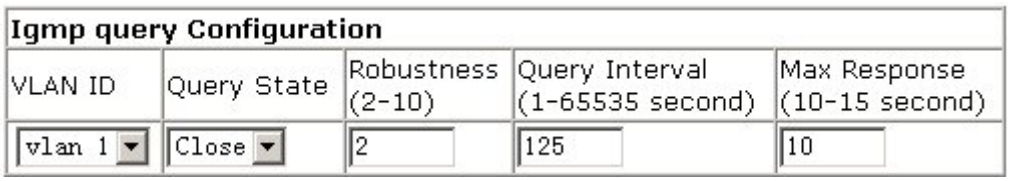
Query State – query state: open or close. See the equivalent CLI command at 7.2.2.6

Robustness – Robustness. See the equivalent CLI command at 7.2.2.7

Query Interval – Query interval. See the equivalent CLI command at 7.2.2.8

Max Response – Maximum response time. See the equivalent CLI command at 7.2.2.9

For example: Select Vlan in the VLAN ID dropdown menu; select Query State as Open; set other attributes, and then click Apply.



7.5.2.2snooping configuration

The explanation of each field is as below:

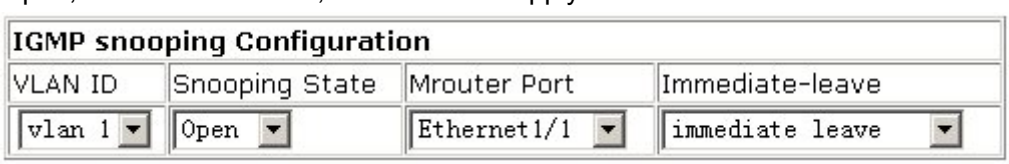
VLAN ID – Configure snooping vlan ID

snooping status – Snooping status: Open or Close. See the equivalent CLI command at 7.2.2.2

mrouter Port - Mrouter Port. See the equivalent CLI command at 7.2.2.3

Immediate-leave - Immediate-leave or no Immediate-leave. See the equivalent CLI command at 7.2.2.5

For example: Select Vlan in the VLAN ID dropdown menu; set snooping status to Open; set other attributes, and then click Apply.



7.5.2.3IGMP configuration

IGMP configuration is shown as below:

IGMP Configuration

VLAN ID	Snooping State	Query State	Robustness	Query Interval	Max Response	Mrouter Port	Immediate-leave
1	Close	Open	2	125	10	(null)	Close
2	Open	Close	0	0	0	(null)	Open

7.5.3 IGMP Snooping static multicast configuration

Click IGMP Snooping static multicast configuration. Users can configure IGMP Snooping static multicast.

7.5.3.1 IGMP Snooping static multicast configuration

The explanation of each field is as below:

VLAN ID – Configure Vlan ID

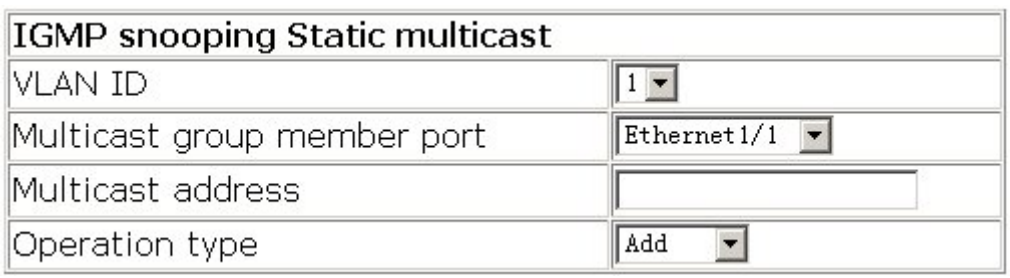
Multicast group member port – Configure multicast group member port

Multicast address – Configure multicast address

Operation type – Add: Add static multicast member port; Remove: Remove static multicast member port.

See the equivalent CLI command at 7.2.2.4

For example: Select Vlan in the VLAN ID dropdown menu; select port in the Multicast group member port dropdown menu; set Multicast address; set Operation type to Add, and then click Apply.



7.5.3.2 IGMP Snooping display

Select a Vlan in the VLAN ID list of static multicast configuration. The IGMP Snooping information is displayed. See the equivalent CLI command at 7.4.1.1

Information display

```
Can not set muti_mac address because igmp snooping is disabled for vlan 1!
IGMP information for VLAN 1:

igmp snooping status                : Enabled
igmp snooping vlan status           : Disabled
igmp snooping vlan mrouter port     : (null)
igmp snooping vlan mrouter present  : No
igmp snooping vlan immediate leave  : No
igmp snooping vlan query            : Enabled
igmp snooping vlan robustness       : 2
igmp snooping vlan query interval   : 125
igmp snooping vlan query max response time: 10
igmp snooping vlan query TX         : 9
igmp snooping vlan query SX         : 0
igmp snooping multicast information  :
MAC address          Member port list
-------------------------------------------------------------------------------
01- 00- 5E- 00- 00- 09       Ethernet1/7
-------------------------------------------------------------------------------

Sort by port:

Port          State             Type              Group Address    Life
-------------------------------------------------------------------------------
Ethernet1/7     MEMBERS_PRESENT       Snoop_Group_Addr     224.0.0.9
180
```

Chapter 8 802.1X CONFIGURATION

8.1 802.1X Introduction

IEEE 802.1X is a kind of port-based network access control technology. The access equipment is authenticated and controlled at the physical access level of LAN equipment. The physical access level used here means the ports of switch equipment. If the user equipment connected to such kind of ports pass the authentication, then the resources of LAN is available to be visited; if the user equipment connected to such kind of ports does not pass the authentication, then the resources of LAN is not available to be visited, which is equal to physical disconnection.

IEEE 802.1x defines the port-based network access control protocol. It shall be noted that the protocol is applicable not only to access equipment, but also to the point-to-point connection modes between ports. The ports may be physical ports or logical ports. The typical application mode: a physical port of switch is connected to only one terminal device (based on physical port).

802.1x system structure as follows:

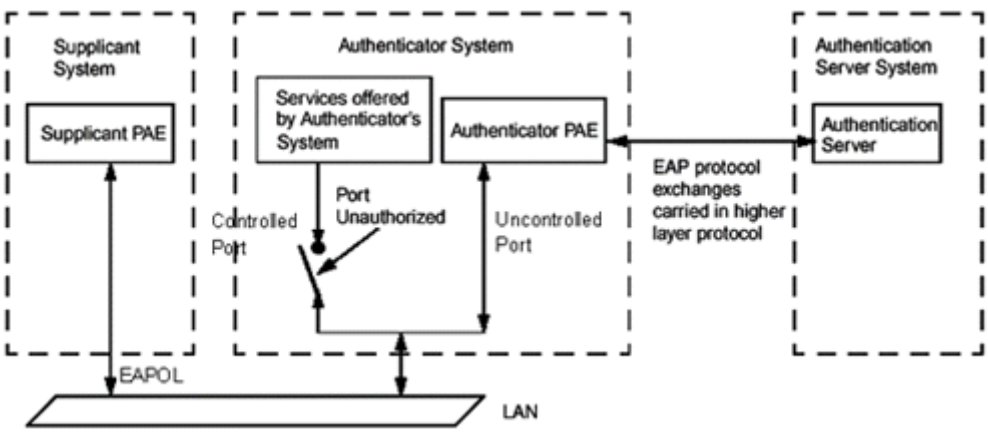


Figure 8-1 802.1x system structure

As the above figure shows, IEEE 802.1x system structure including three parts:

- Supplicant System, user access equipment
- Authenticator System, access control unit;
- Authentication Server System, authentication server

EAPOL protocol defined in 802.1x is adopted between user access equipment (PC) and access control unit (access switch); EAP protocol is also adopted between access control unit and authentication server. Authentication data is sealed in EAP messages, which are included in other high-layer protocol messages, such as RADIUS, so as to reach authentication server through complex network.

The port-based network access control classifies the ports where equipment end provide services to customer end into two virtual ports: controlled port and uncontrolled port. Uncontrolled ports are in bi-directional link state all the time, and used for forwarding EAP messages. Under the authorization state, controlled ports are in link state and are used for forwarding business messages; if the controlled port is not in authorization state, then it will be closed, and no messages may be forwarded.

The Edge-Core switch acts as an access control unit in the 802.1x application environment; user access equipment is equipment with 802.1x customer end software; authentication server generally resides in the AAA center of operators, and Radius server is adopted.

If there are several user access equipments connected to a physical port, the port-based 802.1x authentication fails to distinguish them, which leads to discounted authentication function. The Ede-Core switch realizes the MAC address based 802.1x authentication with stronger performance concerning safety and management. With respect to the user access equipment under a same physical port, if it passes the authentication, the network may be accessed; if it fails to pass the authentication, then the network may not be accessed. Even though there are more than one terminals connected to a physical port of access equipment, the Edge-Core switch is still able to authenticate and manage the user access equipment separately.

The maximum number of authenticated users of this Edge-Core switch is 4000. However, it is recommended the number of authenticated users not exceed 2000.

8.2 802.1X Configuration

8.2.1 802.1X Configuration Task Sequence

1. Enable switch 802.1x function
2. Access control unit property configuration

1) Configure port authorization status

2) Configure port access control method: base on MAC address or base on port

3) Configure switch 802.1x extend function

3. The configuration of something about user access equipment（not required）

4. The configuration of something about RADIUS server

1) Configure RADIUS authentication key

2) Configure RADIUS server

3) Configure RADIUS service parameter

1.Enable switch 802.1x function

Command	**Explanation**
Global configuration mode	
aaa enable **no aaa enable**	Enable switch AAA authentication function; use the “no” command to disable switch AAA authentication function .
aaa-accounting enable **no aaa-accounting enable**	Enable switch accounting function; use the “no” command to disable switch accounting function.
dot1x enable **no dot1x enable**	Enable the switch to force client software to use proprietary 802.1x authentication packet format; the “**no dot1x privateclient enable**” command disables the function and allows the client software to use standard 802.1x authentication packet format.

2.access control unit property configuration

1) Configure port authorize status

Command	Explanation
port configuration mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Configure port 802.1x authorize status; use the “no” command to restore default configuration.
port configuration mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Configure port 802.1x authorize status; use the “no” command to restore default configuration.

2) Configure port access control method

Command	Explanation
port configuration mode	
dot1x port-method {macbased | portbased} **no dot1x port-method**	Configure port access control method; use the “no” command to restore the access control method which base on MAC address.
dot1x max-user <*number*> **no dot1x max-user**	Configure the maximum user for port; Use the “no” command to restore default which is one user.

3) Configure switch 802.1x extend function

Command	Explanation
Global configuration mode	
dot1x macfilter enable **no dot1x macfilter enable**	Enable switch 802.1x address filter function; use the “no” command to disable 802.1x address filter function .
dot1x accept-mac <*mac-address*> [interface <*interface-name*>] **no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**	Add 802.1x address filter table item; use the “no” command to remove 802.1x address filter table item.
dot1x eapor enable **no dot1x eapor enable**	Enable switch EAP relay authentication method; use the “no” command to adopt EAP local terminative authentication method.

3. Some interrelated configuration about Supplicant

Command	Explanation
Global configuration mode	
dot1x max-req <*count*> **no dot1x max-req**	Configure the maximum times of sending EAP-request/MD5 frame when switch did not receive suppliant response before reload authentication; use the “no” command to restore default.
dot1x re-authentication **no dot1x re-authentication**	Configure the permission of re-authentication for suppliant; use the “no” command to close this function.
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	Configure the timeout of quiet-period for the port; use the “no” command to restore default.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Configure the timeout interval of switch suppliant re-authentication; use the “no” command to restore default.

dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	Configure the timeout interval of switch resending EAP-request/identity frame to suppliant; use the "no" command to restore default.
privileged configuration mode	
dot1x re-authenticate [interface <*interface-name*>]	Configure the 802.1x re-authentication to all port or some specific port （not need to wait timeout）.

4. Some interrelated configuration about Authentication Server（RADIUS server）

1) Configure RADIUS authentication key

Command	**Explanation**
Global configuration mode	
radius-server key <*string*> **no radius-server key**	Configure RADIUS server authentication key; use the "no" command to remove RADIUS server authentication key.

2) Configure RADIUS Server

Command	**Explanation**
Global configuration mode	
radius-server authentication host <*IPaddress*> [[port {<*portNum*>}] [primary]] **no radius-server authentication host <*IPaddress*>**	Configure RADIUS authentication server IP address and monitor port ID; use the "no" command to remove RADIUS server.
radius-server accounting host <IPaddress> [[port {<*portNum*>}] [primary]] **no radius-server accounting host <*IPaddress*>**	Configure RADIUS accounting server IP address and monitor port ID; use the "no" command to remove RADIUS server.

3) Configure RADIUS service parameter

Command	**Explanation**
Global configuration mode	
radius-server dead-time <*minutes*> **no radius-server dead-time**	Configure the dead-time for RADIUS server; use the "no" command to restore default configuration.

radius-server retransmit *<retries>* **no radius-server retransmit**	Configure RADIUS retransmit times; use the "no" command to restore default configuration.
radius-server timeout *<seconds>* **no radius-server timeout**	Configure RADIUS server timeout timer; use the "no" command to restore default configuration.

8.2.2 802.1X Configuration Command

8.2.2.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enable switch AAA authentication function; use the "no" command to disable AAA authentication function .

Command mode : global configuration mode

Parameter: None

Default: switch AAA authentication function is not enabled

Instructions: If you want to achieve switch 802.1x authentication function, must enable switch AAA authentication function .

Example: enable switch AAA function

Switch(Config)#aaa enable

8.2.2.2 aaa-accounting enable

Command: aaa-accounting enable

no aaa-accounting enable

Function: Enable switch AAA accounting function; use the "no" command to disable AAA accounting function.

Command mode: global configuration mode

Default: switch default without enable AAA accounting function.

Instructions: After enabling the switch accounting function, switch accounting the authentication according to the port flow information or online time. While accounting is starting, the switch sends "start accounting" message to Radius accounting server; and send "accounting" message to online users every other 5 seconds. When accounting stops, it will send "accounting stop" message to Radius accounting server. Note: Only when accounting function is enabled, can the switch inform Radius accounting server and

while the user is offline, an “offline” message will not inform Radius authentication server.

Example: Enable the switch AAA accounting function.

Switch(Config)#aaa-accounting enable

8.2.2.3 dot1x accept-mac

Command: dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

Function: adds one MAC address list to dot1x address filter table. If specify port, the add list only be suitable for specific port; if not specify port, the add list may be suitable for all port; use the “no” command to remove address filter list of dot1x.

Parameter: <*mac-address*>is MAC address; <*interface-name*>is interface name and interface IID;

Command mode: global configuration mode

Default: None.

Instructions: The switch dot1x address filter function is according to MAC address filter list to achieve, dot1x address filter list manual add or remove by user. If specified port while add dot1x address filter list, this address filter list is only suitable for this port; If not specified port while add, this address filter list suitable for all switch port. When switch dot1x address filter function is enable, switch filter the authentication MAC address, Only the authentication requirement which from dot1x address filter list will be accept, otherwise will be refuse.

Example: Add MAC address 00-01-34-34-2e-0a to Ethernet 1/5 filter list.

Switch(Config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5

8.2.2.4 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Configure switch to adopt EAP relay authentication; use the “no” command to configure switch to adopt EAP local terminating authentication .

Command mode: global configuration mode

Default: switch adopt EAP relay authentication.

Instructions: it may use Ethernet or PPP method to connect between switch and Radius authentication server. If use Ethernet connection between switch and Radius authentication server, the switch needs to adopt EAP relay authentication (that is EAPoR authentication); If using PPP connection between switch and Radius authentication server, the switch needs to adopt EAP local terminating authentication (that is CHAP authentication. According to the different method between switch and authentication server, the switch should adopt different authentication methods to authenticate.

Example: Configure switch to adopt EAP local terminating authentication.

Switch(Config)#no dot1x eapor enable

8.2.2.5 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enable switch global and port 802.1x function; use the “no” command to disable 802.1x function .

Command mode: global configuration mode and port configuration mode

Default: switch without enable 802.1x function in global mode; if switch enables 802.1x function in global, then the port default without enable 802.1x function.

Instructions: If you want to make 802.1x authentication for a port, enable 802.1x function in global mode first, then enable 802.1x function in the corresponding port. Note: If the port has enabled Spanning Tree, enabled mac binding, is a Trunk port, or is member of port aggregation group, then you must disable Spanning Tree function of that port, or disable mac binding, or change the port as an access port, or cancel its status as a port of an aggregation group, otherwise you cannot enable 802.1x function in that port.

Example: Enable switch 802.1x function, and enable port 1/12 802.1x function.

Switch(Config)#dot1x enable

Switch(Config)#interface ethernet 1/12

Switch(Config-Ethernet1/12)#dot1x enable

8.2.2.6 dot1x privateclient enable

Command: dot1x privateclient enable

no dot1x privateclient enable

Function: Enable the switch to force client software to use proprietary 802.1x authentication packet format; the “**no dot1x privateclient enable**” command disables the function and allow the client software to use standard 802.1x authentication packet format.

Command mode: Global Mode

Default: Proprietary authentication is not supported by the switch.

Usage Guide: To implement an overall solution, Edge-Core proprietary IEEE 802.1x authentication packets support must be enabled in the switch, otherwise many application would not be available. Standard 802.1x client would not be authenticated if Edge-Core proprietary 802.1x authentication packet format is enforced for client software by the switch.

Example: Enable the switch to force client software to use Edge-Core proprietary 802.1x authentication packet format.

Switch(Config)#dot1x privateclient enable

8.2.2.7 dot1x macfilter enable

Command: dot1x macfilter enable

no dot1x macfilter enable

Function: Enable switch dot1x address filter function; use the “no” command to disable dot1x address filter function.

Command mode: global configuration mode

Default: switch disable dot1x address filter function.

Instructions: While enable switch dot1x address filter function, switch will filter authentication MAC address, only the authentication requirement which from dot1x address filter list will be accepted.

Example: Enable switch MAC address filter function.

Switch(Config)#dot1x macfilter enable

8.2.2.8 dot1x max-req

Command: dot1x max-req <*count*>

no dot1x max-req

Function: Configure sending EAP-request/MD5 frame maximum times before switch did not receive suppliant response and restart authentication; use the “no” command to restore default.

Parameter: <*count*> is the times of sending EAP-request/ MD5 frame, The range: 1~10.

Command mode: global configuration mode

Default: Maximum is 2 times.

Instructions: When user configure the maximum times of sending EAP-request/ MD5 frame, it is suggested to use default value.

Example: Change the maximum times of EAP-request/ MD5 frame as 5 times.

Switch(Config)#dot1x max-req 5

8.2.2.9 dot1x max-use

Command: **dot1x max-user <*number*>**

no dot1x max-user

Function: Configure the permission maximum user for specific port; use the “no” command to restore default.

Parameter: <*number*> is the maximum permission user amount, The range: 1~254.

Command mode: port configuration mode.

Default: Every port default user is 1.

Instructions: This command is valid only when the port adopts the access control method which is based on MAC address, if the authentication MAC address quantity exceeds the maximum permission access user quantity, the exceed users will not be able to access network.

Example: Configure port 1/3 maximum permission to allow access 5 users.

Switch(Config-Ethernet1/3)#dot1x max-user 5

8.2.2.10 dot1x port-control

Command: dot1x port-control {auto|force-authorized|force-unauthorized }
no dot1x port-control

Function: Configure port 802.1x authorize status; use the “no” command to restore default.

Parameter: auto is used to enable 802.1x authentication, confirm the port is in authorized status or unauthorized status according to the authentication information between switch and suppliant; **force-authorized** configures port as authorized status, allow the unauthorized data through this port; **force-unauthorized** configure port as unauthorized status, switch not provide authentication service to suppliant in this port, not permit any data pass across this port.

Command mode: port configuration mode

Default: When enable port 802.1x function, port default is **force-authorized**.

Instructions: If port want to make 802.1x authentication to user, must configure port authentication status as **auto**.

Example: Configure port 1/1 as 802.1x authentication status.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#dot1x port-control auto

8.2.2.11 dot1x port-method

Command: **dot1x port-method {macbased | portbased}**
no dot1x port-method

Function: Configure the specific port access control method; use the “no” command to restore default access control method.

Parameter: macbased base on MAC address access control method; portbased base on port access control method.

Command mode: port configuration mode

Default: port use access control method which base on MAC address in default mode.

Instructions: The security and management of access control method(base on MAC address) is more predominant than the access control method which base on port, suggest using the access control method base on port only in special situation.

Example: Configure port 1/4 adopt access control method which base on port.

Switch(Config-Ethernet1/4)#dot1x port-method portbased

8.2.2.12 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]

Function: Configure the 802.1x re-authenticate to all port or some specific port in time, not need to wait for time to expire.

Parameter: <*interface-name*>is port ID, if there's no parameter, it means all port.

Command mode: privilege configuration mode

Instructions: This command which belong to privilege mode, after configured this command, switch re-authenticate to client at once, not need to wait re-authenticate clock expire. After authenticated, this command will be invalid.

Example: Re-authenticate port 1/8 in time.

Switch#dot1x re-authenticate interface Ethernet 1/8

8.2.2.13 dot1x re-authentication

Command: dot1x re-authentication

no dot1x re-authentication

Function: Configure to allow re-authentication to suppliant periodicity; use the "no" command to disable this function.

Command mode: global configuration mode

Default: The periodicity re-authentication function is disabled in default mode.

Instructions: When enable periodicity re-authentication function to suppliant, switch will periodicity re-authentication to suppliant. Normally, suggest not enable periodicity re-authentication function.

Example: enable periodicity re-authentication function to suppliant.

Switch(Config)#dot1x re-authentication

8.2.2.14 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>

no dot1x timeout quiet-period

Function: Configure the port quiet-period time after suppliant authentication failure; use the "no" command to restore default.

Parameter: <*seconds*>is port keep quiet-period status time length value, unit is second, The range: 1~65535.

Command mode: global configuration mode

Default: Default is 10 seconds.

Instructions: Suggest using default item.

Example: Configure quiet-period time as 120 seconds.

Switch(Config)#dot1x timeout quiet-period 120

8.2.2.15 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>

no dot1x timeout re-authperiod

Function: Configure switch re-authenticate time interval to supplicant; use the “no” command to restore default.

Parameter: <*seconds*>re-authenticate time interval, unit is second, The range: 1~65535.

Command mode: global configuration mode

Default: Default is 3600 seconds.

Instructions: When modify switch re-authenticate time interval to supplicant, must enable dot1x re-authentication first. If did not configure switch re-authenticate function, the configured time interval of switch re-authenticate to supplicant will not be effective.

Example: Configure re-authentication time as 1200 seconds.

Switch(Config)#dot1x timeout re-authperiod 1200

8.2.2.16 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>

no dot1x timeout tx-period

Function: Configure the time interval which of switch retransmit EAP-request/identity frame to suppliant; use the “no” command to restore default.

Parameter: <*seconds*>is the time interval of retransmit EAP request frame, unit is second, The range: 1~65535.

Command mode: global configuration mode

Default: Default is 30 seconds.

Instructions: suggest using default value.

Example: Modify the retransmit EAP request frame time interval as 1200 seconds.

Switch(Config)#dot1x timeout tx-period 1200

8.2.2.17 radius-server accounting host

Command: radius-server accounting host <*ip-address*> [port <*port-number*>]

[primary]no radius-server accounting host <*ip-address*>

Function: Configure RADIUS accounting server IP address and monitor port ID; use the “no” command to remove RADIUS accounting server .

Parameter: <*ip-address*> server IP address; **<*port-number*>** is server monitor port ID, The range: 0~65535; **primary** is primary server, when configure RADIUS server, may configure many servers, when not configure **primary**, finding usable RADIUS server

according to configuration gradation; if configure **primary**, will use this RADIUS server first.

Command mode: global configuration mode

Default: system without configure RADIUS accounting server.

Instructions: This command for specify accounting RADIUS server IP address and port ID which connect with switch, may configure many command. The parameter<*port-number*>for specify accounting port ID, this port ID must be the same as the accounting port ID which in specific RADIUS server, default is 1813, if configure the port ID as 0, accounting port will random produce, may cause configuration invalid. This command may configure many command over and over for specify many RADIUS server which make communication relationship with switch, switch will send accounting message to all accounting server which has configured, these configured accounting server work as backup server each other. If configure primary, will make this RADIUS server to work as primary server.

Example: Configure RADIUS accounting server IP address as 100.100.100.60, port ID as 3000, and word as primary server.

Switch(Config)#radius-server accounting host 100.100.100.60 port 3000 primary

8.2.2.18 radius-server authentication host

Command: radius-server authentication host <*ip-address*> [port <*port-number*>] [primary]no radius-server authentication host <*ip-address*>

Function: Configure RADIUS server IP address and monitor port ID; use the “no” command to remove RADIUS authentication server.

Parameter: <*ip-address*> server IP address; **<*port-number*>**is server monitor port ID, The range: 0~65535, the “0” means it’s not work as authentication server; **primary** is primary server.

Command mode: global configuration mode

Default: System without configure RADIUS authentication server .

Instructions: This command for specify authentication RADIUS server IP address and port ID, may configure many of this command. The parameter port for specify authentication port ID, this port ID must be the same as authentication port ID which in specific RADIUS server, default is 1812, if configure the port ID as 0, it consider this specific server has no authentication function. This command may configure many command over and over for specify many RADIUS server which make communication relationship with switch, and the gradation of switch authentication server take the gradation of configuration. If configure primary, it will make this RADIUS server work as primary server.

Example: Configure RADIUS authentication server address as 200.1.1.1.

Switch(Config)#radius-server authentication host 200.1.1.1

8.2.2.19 radius-server dead-time

Command: radius-server dead-time <*minutes*>

no radius-server dead-time

Function: Configure the recover time after RADIUS server dead; use the “no” command to restore default configuration.

Parameter: <*minutes*>is the recover time after RADIUS server dead in minutes, The range: 1~255.

Command mode: global configuration mode

Default: Default is 5 minutes.

Instructions: This command specifies the switch wait time which from “cannot access” status restore to ”be able to access” status of the RADIUS server. When switch checked the server cannot be able to access, switch will configure the server status as invalid status, after exceed the above configuration interval time, system will configure the authentication server status as valid.

Example: Configure RADIUS server dead time as 3 minutes.

Switch(Config)#radius-server dead-time 3

8.2.2.20 radius-server key

Command: radius-server key <*string*>

no radius-server key

Function: Configure RADIUS server (including authentication and accounting) authentication key; use the “no” command to remove RADIUS server of authentication key.

Parameter: <*string*> is RADIUS server authentication key string, range cannot exceed 16 characters.

Command mode: global configuration mode

Instructions: This authentication key for switch configure RADIUS server to authenticate message communication. The configured authentication key must be the same as authentication key which configured in RADIUS server, otherwise it will not make correct RADIUS authenticate and accounting.

Example: Configure RADIUS authentication key as test.

Switch(Config)# radius-server key test

8.2.2.21 radius-server retransmit

Command: radius-server retransmit <*retries*>

no radius-server retransmit

Function: Configure RADIUS authentication message retransmit times; use the “no” command to restore default configuration.

Parameter: <*retries*>is RADIUS server retransmit times, The range: 0~100.

Command mode: global configuration mode

Default: Default is 3 times.

Instructions: After this command specify switch sending data packet to RADIUS server, the times which need to retransmit this data packet when it cannot receive RADIUS server response. When did not receive authentication information from authentication server, need to retransmit AAA authentication request to authentication server. If the server response is still not received after the retransmit AAA request times expires, then it will consider the server as not working and the switch will set this server status as ”cannot access”.

Example: Configure RADIUS authentication message retransmit times as 5 times.

Switch(Config)# radius-server retransmit 5

8.2.2.22 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configure RADIUS server timeout timer; use the “no” command to restore default configuration.

Parameter: <*seconds*> is RADIUS server timeout timer value in seconds, The range: 1~1000.

Command mode: global configuration mode

Default: Default is 3 seconds.

Instructions: This command specifies the time interval of switch to wait for the RADIUS server response. After the switch sends request data packet to RADIUS Server, it wait to receive the relevant response data packet. If did not receive the RADIUS server response within the stated time, it will send request data packet according to the temporal status, or configure the server status as ”cannot access”.

Example: Configure radius server timeout time as 30 seconds.

Switch(Config)# radius-server timeout 30

8.3 802.1X Apply Example

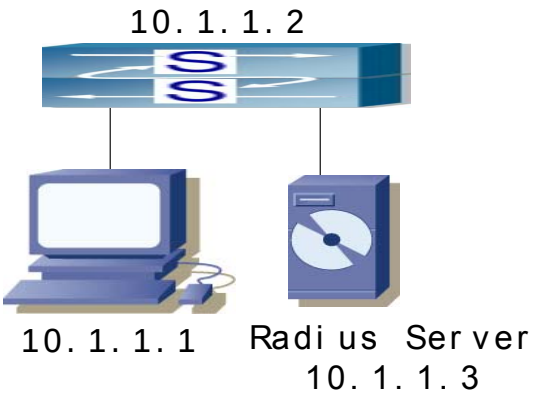


Figure 8-2 IEEE802.1x configuration example topology figure

Computer connect to switch port 1/2, IEEE802.1x authentication function in port 1/2 is enabled, the access method adopt default method is based on MAC address authentication. Configure switch IP address to 10.1.1.2. Connect any port except for port 1/2 to RADIUS authentication server. Configure RADIUS authentication server IP address as 10.1.1.3. authentication, accounting port default is port 1812 and port 1813. Setup IEEE802.1x authentication client software in computer, and achieve IEEE802.1x authentication by using this software.

Configuration steps as below: ↵

Switch(Config)#interface vlan 1↵

Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0↵

Switch(Config-if-vlan1)#exit↵

Switch(Config)#radius-server authentication host 10.1.1.3↵

Switch(Config)#radius-server accounting host 10.1.1.3↵

Switch(Config)#radius-server key test↵

Switch(Config)#aaa enable↵

Switch(Config)#aaa-accounting enable↵

Switch(Config)#dot1x enable↵

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#dot1x enable↵

Switch(Config-Ethernet1/2)#dot1x port-control auto↵

Switch(Config-Ethernet1/2)#exit

8.4 802.1X Trouble Shooting

8.4.1 802.1X Debug and Monitor Command

8.4.1.1 show aaa config

Command: show aaa config

Function: Displays the existing configuration commands while the switch works as RADIUS client.

Command mode: privilege mode

Instructions: Display switch whether is enable aaa authentication, accounting function, and authentication key, authentication, accounting server information, etc.

Example:

Switch#show aaa config（If it is Boolean, 1 means TRUE, 0 means FALSE）

---------- AAA config data ----------

Is Aaa Enabled = 1
Is Account Enabled= 1
MD5 Server Key = aa
authentication server sum = 2
authentication server[0].Host IP = 30.1.1.30
.Udp Port = 1812
.Is Primary = 1
.Is Server Dead = 0
.Socket No = 0
authentication server[1].Host IP = 192.168.1.208
.Udp Port = 1812
.Is Primary = 0
.Is Server Dead = 0
.Socket No = 0
accounting server sum = 2
accounting server[0].Host IP = 30.1.1.30
.Udp Port = 1813
.Is Primary = 1
.Is Server Dead = 0

.Socket No = 0

accounting server[1].Host IP = 192.168.1.208

.Udp Port = 1813

.Is Primary = 0

.Is Server Dead = 0

.Socket No = 0

Time Out = 3

Retransmit = 3

Dead Time = 5

Account Time Interval = 0

Display Content	**Description**
Is Aaa Enabled	Display AAA authentication function whether is enable. 1 means enable; 0 means disable;
Is Account Enabled	Display AAA accounting function whether is enable. 1 means enable; 0 means disable;
MD5 Server Key	Display RADIUS server authentication key;
authentication server sum	Authentication server sum;
authentication server[X].Host IP **.Udp Port** **Is Primary** **Is Server Dead** **.Socket No**	Display authentication server ID and corresponding IP address, UDP port ID, whether is Primary server, the server whether is dead、Socket No;
accounting server sum	Accounting server sum;
accounting server[X].Host IP **.Udp Port** **.Is Primary** **.Is Server Dead** **.Socket No**	Display accounting server ID and corresponding IP address, UDP port ID, whether is Primary server, whether is dead, Socket No;
Time Out	Display RADIUS server timeout timer;
Retransmit	Display RADIUS server authentication message retransmit times;
Dead Time	Display RADIUS recovery time after RADIUS server dead;
Account Time Interval	Display accounting time interval

8.4.1.2 show aaa authenticated-user

Command: show aaa authenticated-user

Function: Displays the online authenticated users.

Command mode: privilege mode

Instructions: Other online user information is typically used for technical support engineers for diagnosis and troubleshooting.

Example:

Switch#show aaa authenticated-user

---------- authenticated users ----------

User-name	Retry-time	Radius-ID	Port	Eap-ID	Chap-ID	Mem-Addr	WaitingNum
bb	0	4	2	0	1	16652824	0

8.4.1.3 show aaa authenticating-user

Command: show aaa authenticating-user

Function: Displays the authenticating user.

Command mode: privileged mode

Instructions: Normally use is for information of authenticating users, technical support engineers can use other information for trouble diagnosis and troubleshooting.

Example:

Switch#show aaa authenticating-user

---------- authenticating users ----------

User-name	Retry-time	Radius-ID	Port	Eap-ID	Chap-ID	Mem-Addr	WaitingNum
bb	0	4	2	1	0	16652824	0

8.4.1.4 show radius count

Command: show radius {authencated-user|authencating-user} count

function : Displays radius authentication user statistics information.

Parameter: authenticated-user: ddisplays the online authenticated authentication user; authenticating-user: is the authenticating user.

Command mode: privileged configuration mode

Instructions: You may check radius authentication user statistics information by using “show radius count” command.

Example:

1. Show radius authenticated-user statistics information.

Switch #show radius authenticated-user count

---------- Radius user statistic----------

The authenticated online user num is: 1

The total user num is: 1

2. Show radius authenticating-user statistics information and others

Switch #sho radius authencating-user count

---------- Radius user statistic----------

The authenticating user num is: 0

The stopping user num is: 0

The stopped user num is: 0

The total user num is: 1

8.4.1.5 show dot1x

Command: show dot1x [interface <*interface-list*>]

Function: Display dot1x parameter information, if add parameter information, it will display dot1x status of relevant port.

Parameter: <*interface-list*> is port list. If there's no parameter, will display all port information

Command mode: privilege configuration mode

Instructions: By using show dot1x command you may check port dot1x relevant parameters and port dot1x information.

Example:

1.Display switch dot1x global parameters information.

Switch#show dot1x

Global 802.1x Parameters

reauth-enabled	no
reauth-period	3600
quiet-period	10
tx-period	30
max-req	2
authenticator mode	passive

Mac Filter Disable

MacAccessList :

dot1x-EAPoR Enable

802.1x is enabled on ethernet 1

Authentication Method: Port based

Status	Authorized
Port-control	Auto
Supplicant	00-03-0F-FE-2E-D3

Authenticator State Machine

State	Authenticated

Backend State Machine

State	Idle

Reauthentication State Machine

State	Stop

Display Content	Explanation
Global 802.1x Parameters	Global 802.1x parameters information
reauthenabled	switch whether is enable authentication function
reauth-period	Re-authentication time interval
quiet-period	Quiet-period time interval
tx-period	EAP data packet retransmit time interval
max-req	EAP data packet retransmit times
authenticator mode	switch authenticator mode
Mac Filter	switch whether is enable dot1x address filter function
MacAccessList :	Dot1x address filter list
dot1x-EAPoR	switch adoptive authentication method (EAP relay, EAP local terminating)
802.1x is enabled on ethernet 1	Display port dot1x whether is enable
Authentication Method:	port authentication method (base on MAC, base on port)
Status	port authentication status
Port-control	port authorization status
Supplicant	authentication MAC address
Authenticator State Machine	Authenticator state machine status

Backend State Machine	Backend state machine status
Reauthentication State Machine	Reauthentication state machine status

8.4.1.6 debug aaa

Command: debug aaa

no debug aaa

Function: Enable aaa debug information; use the “no” command to close aaa debug information.

Command mode: privilege configuration mode

Parameter: None

Instructions: Enables aaa debug information, may check the negotiation process of Radius protocol, it’s conduce to debug trouble when have troubles.

Example: Enable aaa debug information.

Switch#debug aaa

8.4.1.7debug dot1x

Command: debug dot1x

no debug dot1x

Function: Enables dot1x debug information; use the “no” command to close dot1x debug information.

Command mode: privileged configuration mode

Parameter: None

Instructions: Enable dot1x debug information, may check the negotiation process of dot1x protocol, it’s conduce to debug trouble when have troubles.

Example: Enable dot1x debug information.

Switch#debug dot1x

8.4.2 802.1X Troubleshooting

When using 802.1x and the ports usually fail to configure 802.1x; or the authentication state of 802.1x is “auto”, after the user run the “supplicant” software of 802.1x, the port still fails to be in state where authentication is passed. The possible reasons and solutions are as follows:

- When failing to configure the 802.1x, examine whether spanning-tree is being run at the switch ports, and whether the mac port is bound or has been set as trunk

port. For enabling the 802.1x authentication function, it is necessary to disable the trunk functions of the port.

- If the switch is configured correctly and the authentication is still not passed, it is recommended to examine whether links are established between the switch and RADIUS server, the switch and 802.1x; the configuration of switch port VLAN should also be examined.
- The event log of RADIUS server is examined for determining the reasons of problems. Failures and their reasons are recorded in the event log. If the event log indicates that the password of authenticator is incorrect, the radius-server parameter shall be changed; if the vent log indicates that there is no authenticator, it shall be added to RADIUS server; if the event log prompt that there is no the log user, the log name and password are incorrect. Correct ones shall be entered.
- If frequent operations are conducted on RADIUS data, for example frequent calling of several commands of “show aaa”, the share of RADIUS data may cause that the user fails to pass authentication. It is recommended to reduce operations on RADIUS data. The user may be forced offline during authentication again because over frequent use of RADIUS data. If users make authentication requests or online users are authenticated again, it is recommended to reduce operations on RADIUS.

8.5 WEB Management

Click Authentication configuration, open authentication configuration management list, user may configure switch 802.1x authentication function.

8.5.1RADIUS client configuration

Click Authentication configuration, RADIUS client configuration, open Radius client configuration management list, user may configure switch Radius client.

8.5.1.1 RADIUS global configuration

Click Authentication configuration, RADIUS client configuration, RADIUS global configuration. You may configure Radius global configuration information:

- Authentication status – Enable, disable switch AAA authentication function. Disable radius Authentication, disable AAA authentication function; Enable radius Authentication, enable AAA authentication function. It is equivalent to CLI command 8.2.2.1.
- Accounting Status – Enable, disable switch AAA accounting function. Disable Accounting, disable accounting function; Enable Accounting, enable accounting function. It is equivalent to CLI command 8.2.2.2.
- RADIUS key - Configure the authentication of RADIUS server（including

authentication and accounting）It is equivalent to CLI command 8.2.2.19.

- System recovery time (1-255 minute) - Configure the recover time after RADIUS server dead. It is equivalent to 8.2.2.18.
- RADIUS Retransmit times(0-100) - Configure RADIUS authentication message retransmit times. It is equivalent to CLI command 8.2.2.20.
- RADIUS server timeout (1-1000 second) - Configure RADIUS server timeout timer. It is equivalent to CLI command 8.2.2.20.

Choose Authentication status as Enable radius Authentication, select Accounting Status as Enable Accounting, Configure RADIUS key as “aaa”, Configure System recovery time as 10 seconds, Configure RADIUS Retransmit times as 5 times, Configure RADIUS server timeout as 30 seconds, Click Apply button, these configuration will be applied to switch.

RADIUS configuration	
Authentication status	☑ Enabled
Accounting Status	☑ Enabled
RADIUS key	aaa
System recovery time (1-255 minute)	10
RADIUSRetransmit times(0-100)	5
RADIUS server timeout(1-1000 second)	30

8.5.1.2 RADIUS authentication configuration

Click Authentication configuration, RADIUS client configuration, RADIUS authentication configuration. Configure RADIUS authentication server IP address and monitor port ID. It is equivalent to CLI command 8.2.2.17.

- Authentication server IP ---Server IP address.
- Authentication server port(optional) ---Is server monitor port ID, The range: 0~65535, the “0” means it’s not work as authentication server.
- Primary authentication server –--- Primary Authentication server, is primary server; Non-Primary Authentication server, is non-primary server.
- Operation type – Add authentication server, add authentication server; Remove authentication server, remove authentication server.

Configure Authentication server IP as 10.0.0.1, Authentication server port as default port, select Primary Authentication server, choose Operation type as “Add authentication server”, Click Apply button that is added an authentication server.

RADIUS authentication server configuration	
Authentication server IP	10 . 0 . 0 . 1
Authentication server port(optional)	
Primary authentication server	Primary authentication server
Operation type	Add authenticating server

RADIUS server configuration list		
Server IP	Port num	Primary server

8.5.1.3 RADIUS accounting configuration

Click Authentication configuration, RADIUS client configuration, RADIUS accounting configuration. Configure RADIUS accounting server IP address and monitor port ID. It is equivalent to CLI command 8.2.2.16.

- Accounting server IP - server IP address.
- Accounting server port (optional) – is the accounting server port ID, The range: 0~65535, the “0” means that it’s not work as authentication server.
- Primary accounting server – Primary Accounting server, is primary server; Non-Primary Accounting server, is non-primary server.
- Operation type – Add accounting server, add accounting server; Remove accounting server, remove accounting server

Configure Accounting server IP as 10.0.0.1, accounting server port as default port, choose Primary accounting server, choose Operation type as “Add accounting server”, Click Apply button that is added an accounting server.

RADIUS accounting server configuration	
Accounting server IP	10 . 0 . 0 . 1
Accounting server port (optional)	
Primary accounting server	Primary accounting server
Operation type	Add accounting server

RADIUS accounting server configuration list		
server IP	port num	Primary server

8.5.2 802.1X Configuration

Click Authentication configuration, 802.1X configuration, open 802.1x function configuration management list, user may configure switch 802.1x function.

8.5.2.1 802.1X Configuration

Click Authentication configuration, 802.1X configuration, 802.1X configuration. Configure 802.1x global configuration:

- 802.1x status – Enable, disable switch 802.1x function. It is equivalent to CLI command 8.2.2.5.
- Maximum retransmission times of EAP-request/identiry (1-10 second) - Configure sending EAP-request/MD5 frame maximum times before switch did not receive suppliant response and restart authentication. It is equivalent to CLI command 8.2.2.7.
- Reauthenticate client periodically ---permit, forbid to make seasonal re-authentication for suppliant. It is equivalent to CLI command 8.2.2.12.
- Hold down time for authentication failure (1-65535 second) -Configure suppliant quiet-period status time after authentication failure, the same as CLI command 8.2.2.13.
- Reauthenticate client interval(1-65535 second) - Configure time interval of switch reauthentication client. It is equivalent to CLI command 8.2.2.14.
- Resending EAP-request/identity interval(1-65535 second) - Configure time interval of switch retransfer EAP-request/identity frame to suppliant. It is equivalent to CLI command 8.2.2.15.
- EAP relay authentication mode - Configure switch to adopt EAP relay method to make authentication; use the “no” command to configure switch to adopt EAP local terminating method to make authentication. It is equivalent to CLI command 8.2.2.4.
- MAC filtering – Enable, disable switch dot1x address filter function. It is equivalent to CLI command 8.2.2.6.

Choose 802.1x status as Enable 802.1x, Configure Maximum retransmission times of EAP-request/identiry as 1, choose Reauthenticate client periodically as Disable Reauthenticate, Configure Hold down time for authentication failure as 1, Configure Reauthenticate client interval as 1, Configure Resending EAP-request/identity interval as 1, Choose EAP relay authentication mode as forbid, choose MAC filtering as forbid, Click Apply button to apply the configuration to switch.

802.1X	
802.1x status	☐ Enabled
Maximum retransmission times of EAP-request/identiry(1-10 second)	2
Reauthenticate client periodically	☐ Enable
Holddown time for authentication failure(1-65535 second)	10
Reauthenticate client interval(1-65535 second)	3600
Resending EAP-request/identity interval(1-65535 second)	30
EAP relay authentication mode	forbid
MAC filtering	forbid

8.5.2.2 802.1X port authentication configuration

Click Authentication configuration, 802.1X configuration, 802.1X port authentication configuration. Configure port 802.1xFunction:

- Port – assign port
- 802.1x status – port 802.1x status, Enable, 802.1x function is enable; Close, 802.1x function is close, the same as CLI command 8.2.2.5.
- Authentication type - Configure port 802.1x authentication status. Auto means enable 802.1x authentication, According to switch and suppliant authentication information to confirm port is in authenticated status or unauthenticated status; force-authorized is configure port as authenticated status, allow the unauthenticated data to pass across the port; force-unauthorized is configure port unauthenticated status, switch not provide suppliant authentication service in this port, not permit any port pass across this port, the same as CLI command 8.2.2.9.
- Authentication mode -Configure access control method for specific port. Mac-based is access control method which base on MAC address; port based access control method which base on port, the same as CLI command 8.2.2.10.
- Port maximum user(1-254) - Configure the permission maximum user for specific port, the same as CLI command 8.2.2.8.

Choose port Ethernet1/1, choose 802.1x status as Enabled, choose Authentication type as auto, choose Authentication mode as port based, Configure Port maximum user as 10, Click Set button, and apply this configuration to switch.

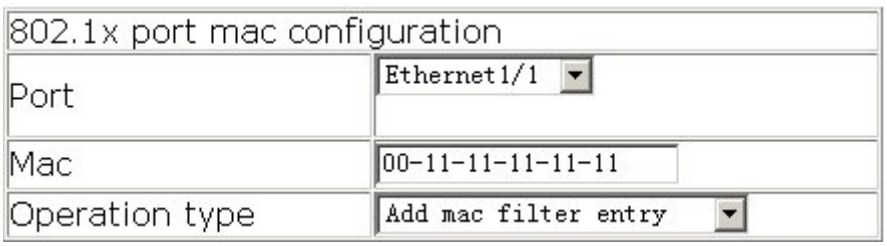
802.1x port configuration	
Port	Ethernet1/1
802.1x status	☑ Enabled
Authentication type	Auto(802.1X)
Authentication mode	Port-based
Port maximum user(1-254)	0

8.5.2.3 802.1x port mac configuration

Click Authentication configuration, 802.1X configuration, 802.1x port mac configuration. Add a MAC address table to dot1x address filter. It is equivalent to CLI command 8.2.2.3.

- Port –If specify port, the added list only suitable for specific port, specify All Ports, the added list suitable for all port.
- Mac – added MAC address
- Operation type – add、remove filter MAC

Choose port Ethernet1/1, Configure MAC as 00-11-11-11-11-11, choose Operation type as Add mac filter entry, Click Apply button, and apply this configuration to switch.

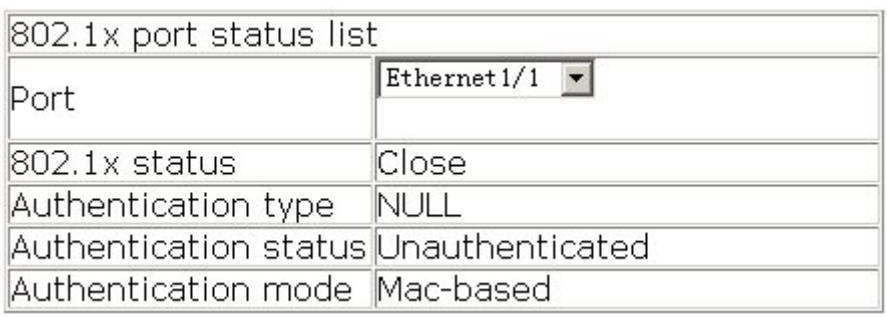


8.5.2.4 802.1x port status list

Click Authentication configuration, 802.1X configuration, 802.1x port status list. Display port 802.1x configuration information, and may re-authentication for the specific port, the same as CLI command 1.2.2.11.

- Port – assign port
- 802.1x status – port 802.1x status
- Authentication type –Authentication type
- Authentication status –Authentication status
- Authentication mode –Authentication mode

Choose port Ethernet1/1, then Click Reauthenticate button, the user in port Ethernet1/1 will be force to make re-authentication.



Chapter 9 ACL Configuration

9.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access through the switches, effectively safeguards the security of networks. The user can lay down a set of rules according to some information specific to the packet, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming or outgoing direction of the switch ports, so that data stream in the specific direction of specified ports must comply with the ACL rules assigned.

9.1.1 Access list

Access list is a sequential collection of conditions that corresponds to a specific rule. Each rule consists of filter information and the action when the rule is matched. Information include in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port. Access list can be categorized by the following criteria:

- Filter information based criterion: IP access list (information of layer 3 and above), MAC access list (layer 2 information), and MAC-IP access list (information of layer 2 and above). The current implementation support IP access list only, the other two functions will be provided later.
- Configuration complexity based criterion: standard and extended, extended mode allow more specific filter information.
- Nomenclature based criterion: numbered and named.

Description of an ACL should cover the above three aspects.

9.1.2 Access-group

When a set of access lists are created, they can be applied to traffic of any direction on all ports. Access-group is the description to a the binding of an access list to the specified direction on a specific port. When an access-group is created, all packets from in the specified direction through the port will be compared to the access list rule to

decide whether to permit or deny access.

9.1.3 Access list Action and Global Default Action

There are two access list action and default action: “permit” or “deny”.
The following rules apply:

- An access list can consist of several rules. Filtering of packets is to compare packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed.
- Global default action applies only to IP packets in the incoming direction on the ports. For non-IP incoming packets and all outgoing packets, the default forward action is “permit”.
- Global default action applies only when packet flirter is enabled on a port, and no ACL is bound to that port, or no binding ACL matches.
- When an access list is bound to the outgoing direction of a port, the action in the rule can only be “deny”.

9.2 ACL configuration

9.2.1 ACL Configuration Task Sequence

1. Configuring access list
   （1） Configuring a numbered standard IP access list
   （2） Configuring an numbered extended IP access list
   （3） Configuring a standard IP access list basing on nomenclature
      a) Create an standard IP access list basing on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   （4） Configuring an extended IP access list basing on nomenclature.
      a) Create an extensive IP access list basing on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
2. Configuring packet filtering function
   (1) Enable global packet filtering function
   (2) Configure default action.

3. Bind access list to a specific direction of the specified port.

1. Configuring access list

(1) Configuring a numbered standard IP access list

Command	Explanation
Global Mode	
access list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} **no access list <*num*>**	Create a numbered standard IP access list, if the access list already exists, then a rule will add to the current access list; the "**no access list <*num*>**" command deletes a numbered standard IP access list.

(2) Configuring a numbered extensive IP access list

Command	Explanation
Global Mode	
access list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Create a numbered ICMP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Create a numbered IGMP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Create a numbered TCP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Create a numbered UDP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.

access list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Create a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
no access list <*num*>	Delete a numbered extensive IP access list

(3)Configuring a standard IP access list basing on nomenclature

a. Create a name-based standard IP access list

Command	Explanation
Global Mode	
access-list ip standard <*name*> **no access-list ip standard <*name*>**	**Create a standard IP access list based on nomenclature; the "no ip access standard <*name*>" command delete the name-based standard IP access list**

b.Specify multiple "permit" or "deny" rules

Command	Explanation
Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any | {host <*sIpAddr*>}}	Create a standard name-based IP access rule; the "no" form command deletes the name-based standard IP access rule

c. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IP ACL Mode	
Exit	Exit name-based standard IP ACL configuration mode

4) Configuring an name-based extended IP access list

a. Create an extended IP access list basing on nomenclature

Command	Explanation
Global Mode	
access-list ip extended <*name*> **no access-list ip extended <*name*>**	Create a extended IP access list basing on nomenclature; the "**no ip access extended <*name*>**" command delete the name-based extended IP access list

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Extended IP ACL Mode	

[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Create an extended name-based ICMP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Create an extended name-based IGMP IP access rule; the "no" form command deletes this name-based extended IP access rule

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Create an extended name-based TCP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Create an extended name-based UDP IP access rule; the "no" form command deletes this name-based extended IP access rule
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Create an extended name-based IP access rule for other IP protocols; the "no" form command deletes this name-based extended IP access rule

c. Exit extended IP ACL configuration mode

Command	Explanation
Extended IP ACL Mode	
Exit	Exit extended name-based IP ACL configuration mode

2. Configuring packet filtering function

(1) Enable global packet filtering function

Command	Explanation
Global Mode	
firewall enable	Enable global packet filtering function

firewall disable	disable global packet filtering function

(2) Configure default action.

Command	Explanation
Global Mode	
firewall default permit	Set default action to “permit”
firewall default deny	Set default action to “deny”

3. Bind access-list to a specific direction of the specified port.

Command	Explanation
Physical Interface Mode	
ip access-group <*name*> {in|out } **no ip access-group <*name*> {in|out}**	Apply an access list to the specified direction on the port; the “**no ip access-group <*name*> {in|out}**” command deletes the access list bound to the port.

9.2.2 ACL Configuration Commands

9.2.2.1 access-list(extended)

Command: access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>]

[tos <*tos*>]

no access-list <*num*>

Function: Create a numbered extended IP access rule for specific IP protocol or all IP protocols; if the numbered extended access list of specified number does not exist, then an access list will be created using this number. The “no” form command deletes a numbered extended IP access list.

Parameter: ***<num>*** is the access table number from 100 to 199; ***<sIpAddr>*** is the source IP address in dot decimal format; ***<sMask >*** is the mask complement of the source IP in dot decimal format; ***<dIpAddr>*** is the destination IP address in dot decimal format; ***<dMask>*** is the mask complement of the destination IP in dot decimal format, 0 for significant bit and 1 for ignored bit; ***<igmp-type>*** is the IGMP type; ***<icmp-type>*** is the ICMP type; ***<icmp-code>*** is the ICMP protocol number; ***<prec>*** is the IP priority from 0 – 7; ***<tos>*** is the tos value from 0 -15; ***<sPort>*** is the source port number from 0 – 65535; ***<dPort>*** is the destination port number from 0 – 65535.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When the user first specifies a specific ***<num>***, the ACL of this number will be created, and entries can be added to that ACL.

Example: Create an extensive IP access list numbered as 110. Deny ICMP packets and allow UDP packets destined for 192.168.0.1, port 32.

Switch(Config)#access list 110 deny icmp any-source any-destination

Switch(Config)#access list 110 permit udp any-source host-destination 192.168.0.1 d-port 32

9.2.2.2 access list(standard)

Command: access list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}

no access list <*num*>

Function: Create a numbered standard IP access list, if the access list already exists, then a rule will add to the current access list; the “**no access list <*num*>**” command deletes a numbered standard IP access list.

Parameter: ***<num>*** is the access list number from 1 to 99; ***<sIpAddr>*** is the source IP address in dot decimal format; ***<sMask >*** is the mask complement for source IP in dot decimal format.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When the user first specifies a specific ***<num>***, the ACL of this number will

be created, and entries can be added to that ACL.

Example: Create a standard IP access list numbered 20, allowing packets from 10.1.1.0/24 and deny packets from 10.1.1.0/16.

Switch(Config)#access list 20 permit 10.1.1.0 0.0.0.255

Switch(Config)#access list 20 deny 10.1.1.0 0.0.255.255

9.2.2.3 firewall

Command: firewall { enable | disable}

Function: Enable or disable firewall.

Parameter: Enable for allow firewall function; disable for prevent firewall action.

Default: The firewall is disabled by default.

Command mode: Global Mode

Usage Guide: Access rules can be configured regardless of firewall status. But the rules can only be applied to the specified direction of specified ports when the firewall is enabled. When the firewall is disabled, all ACL bound to the ports will be deleted.

Example: enable firewall.

Switch(Config)#firewall enable

9.2.2.4 firewall default

Command: firewall default {permit | deny}

Function: set firewall default action.

Parameter: "**permit**" allows packets to pass through; "**deny**" blocks packets.

Command mode: Global Mode

Default: The default action is "permit".

Usage Guide: This command affect incoming IP packets on the port only, other packets are allowed to pass through the switch.

Example: set firewall default action to block packets.

Switch(Config)#firewall default deny

9.2.2.5 access-list ip extended

Command: access-list ip extended <*name*>

no access-list ip extended <*name*>

Function: Create a name-based extended IP access list; the "**no ip access extended <*name*>**" command delete the name-based extended IP access list

Parameter: <*name*> is the name for access list, the character string length is 1 – 8, pure digit sequence is not allowed.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create an extensive IP access list named "tcpFlow".

Switch(Config)# access-list ip extended tcpFlow

9.2.2.6 access-list ip standard

Command: access-list ip standard <*name*>

no access-list ip standard <*name*>

Function: Create a name-based standard IP access list; the "**no ip access standard <*name*>**" command delete the name-based standard IP access list (including all entries).

Parameter: <*name*> is the name for access list, the character string length is 1 – 8.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create an standard IP access list named "ipFlow".

Switch(Config)# access-list ipstandard ipFlow

9.2.2.7 ip access-group

Command: ip access-group [<*num*>|<*acl-name*> { in|out }

no ip access-group <*name*> { in|out }

Function: Apply an access list to the incoming direction on the port; the "**no ip access-group <*name*> {in|out}**" command deletes the access list bound to the port.

Parameter <*name*> is the name for access list; the character string length is 1 – 8.

Command mode: Physical Interface Mode

Default: No ACL is bound by default.

Usage Guide: Only one access rule can be bound to a port, application of access list on the outgoing direction is not supported yet.

Example: Bind access list “aaa” to the incoming direction of the port.
Switch(Config-Ethernet1/1)#ip access-group aaa in

9.2.2.8 permit | deny(extended)

Command: [no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]

Function: Create or delete a name-based extended IP access rule for a specified IP protocol or all IP protocols.

Parameter: <*sIpAddr*> is the source IP address in dot decimal format; **<*sMask* >** is the mask complement of the source IP in dot decimal format; **<*dIpAddr*>** is the destination IP address in dot decimal format; **<*dMask*>** is the mask complement of the destination IP in dot decimal format, 0 for significant bit and 1 for ignored bit; **<*igmp-type*>** is the IGMP type from 0 to 255; **<*icmp-type*>** is the ICMP type from 1 to 255; **<*icmp-code*>** is the ICMP protocol number from 0 to 255; **<*prec*>** is the IP priority from 0 – 7; **<*tos*>** is the tos value from 0 -15; **<*sPort*>** is the source port number from 0 – 65535; **<*dPort*>** is the destination port number from 0 – 65535.

Command Mode: named-based extended IP ACL configuration mode

Default: No IP address is configured by default.

Example: Create an extensive IP access list named “udpFlow”. Deny IGMP packets and allow UDP packets destined for 192.168.0.1, port 32.

Switch(Config)# access-list ip extended udpFlow

Switch(Config-Ext-Nacl-udpFlow)#deny igmp any-source any-destination

Switch(Config-Ext-Nacl-udpFlow)#permit udp any-source host-destination 192.168.0.1

d-port 32

9.2.2.9 permit | deny(standard)

Command: {deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}}
no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}}

Function: Create a standard name-based IP access rule; the “no” form command deletes the name-based standard IP access rule

Parameter: Parameter: **<*sIpAddr*>** is the source IP address in dot decimal format; **<*sMask* >** is the mask complement for source IP in dot decimal format.

Command Mode: named-based standard IP ACL configuration mode

Default: No IP address is configured by default.

Example: Allow packets from 10.1.1.0/24 and deny packets from 10.1.1.0/16.

Switch(Config)# access-list ip standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

9.3 ACL Example

Scenario 1:

The user has the following configuration requirement: port 1/10 of the switch connecting to 10.0.0.0/24 segment, ftp is not desired for the user to use.

Configuration description:

1. Create a proper ACL
2. Configuring packet filtering function
3. Bind the ACL to the port

The configuration steps are listed below:

Switch(Config)#access list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(Config)#firewall enable
Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#ip access-group 110 in
Switch(Config-Ethernet1/10)#exit
Switch(Config)#exit

Configuration result.:

Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.
Switch#show access lists
access list 110(used 1 time(s))
    access list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/10
interface name: Ethernet1/10
     the ingress acl use in firewall is 110.

9.4 ACL Troubleshooting Help

9.4.1 ACL Debug and Monitor Commands

9.4.1.1 show access lists

Command: show access lists [<*num*>|<*acl-name*>]
Function: Displays the access list configured.
Parameter: <*acl-name*> is the specified access list naming string; **<*num*>** is the specified access list number.
Default: N/A.
Command mode: Admin Mode
Usage Guide: When access list name is not specified, all access list will be displayed; used x time（s）indicates the number the ACL is referred to.
Example:
Switch#show access lists
access list 10(used 0 time(s))
    access list 10 deny any-source

access list 100(used 1 time(s))
    access list 100 deny ip any-source any-destination
    access list 100 deny tcp any-source any-destination

Displayed information	Explanation
access list 10(used 0 time(s))	Numbered ACL10, reference time: 1.

access list 10 deny any-source	Deny all IP packets passage.
access list 100(used 1 time(s))	Numbered ACL100, reference time: 1.
access list 100 deny ip any-source any-destination	Deny IP packets of any source addresses and destination addresses.
access list 100 deny tcp any-source any-destination	Deny TCP packets of any source IP addresses and destination IP addresses.

9.4.1.2 show access-group

Command: show access-group [interface <*name*>]

Function: display ACL binding information for the port.

Parameter: <*name*> is the port name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: If no port is specified, then ACL bound in all ports will be displayed.

Example:

Switch#show access-group

interface name: Ethernet1/2

Ingress access-list used is 111.

interface name: Ethernet1/1

Ingress access-list used is 10.

Displayed information	Explanation
interface name: Ethernet1/2	Binding information of port Ethernet1/2.
Ingress access list used is 111.	Numbered extended ACL 111 bound to the incoming direction of port Ethernet1/2.
interface name: Ethernet1/1	Binding information of port Ethernet1/1.
Ingress access list used is 10.	Numbered standard ACL 10 bound to the incoming direction of port Ethernet1/1.

9.4.1.3 show firewall

Command: show firewall

Function: Display packet filtering configuration information.

Parameter: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

Switch#show firewall

Firewall Status: Enable.

Firewall Default Rule: Permit.

Displayed information	Explanation
Firewall Status: Enable.	Enable packet filtering function
Firewall Default Rule: Permit.	The default action for packet filtering is “permit”

9.4.2 ACL Troubleshooting Help

- The check for entries in the ACL is in a top-down order, and ends whenever an entry is matched.
- Default rule will be used only if no ACL is bound to the specific direction of the port, or no ACL entry is matched.
- Applies to IP packets incoming on all ports, and has no effect on other types of packets.
- One port can bind only one incoming ACL.
- The number of ACL that can be successfully bound depends on the content of ACL bound and hardware resource limit. The user will be prompted if ACL cannot be bound due to hardware resource limitation.
- If an access list contains same filtering information but conflicting action rule, binding to the port will fail with an error message. For instance, configuring “permit tcp any-source any-destination” and ”deny tcp any-source any-destination” the same time.
- Virus such as “worm.blaster” can be blocked by configuring ACL to block certain ICMP packets.

9.5 Web Management

Click ACL configuration. The ACL configuration page is shown:

Numeric ACL configuration – Configure Numeric ACL, including standard ACL and extended ACL

ACL name configuration – Configure name ACL, including standard ACL and extended ACL

Filter configuration - Enable filter globally. ACL filter is binded to the port by default.

9.5.1Add standard numeric IP ACL configuration

Click Numeric ACL configuration, Add standard numeric. Users can configure ACL. See the equivalent CLI command at 9.2.2.2

The explanation of each field is as below:

ACL number - ACL number (1 – 99)

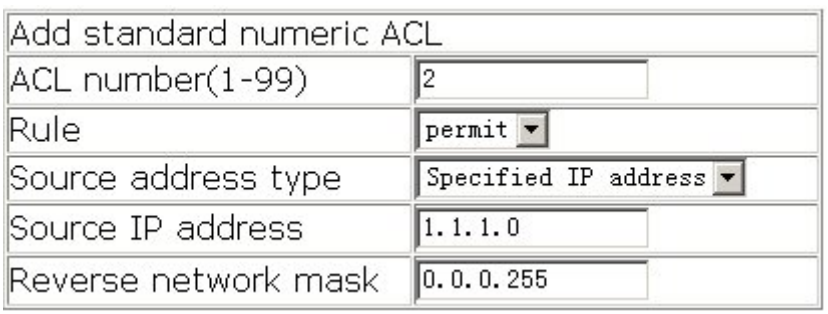
Rule – permit; deny

Source address type - Specified IP address or allow any address

Source IP address - Source IP address

Reverse network mask - Reverse network mask

For example: Add a standard numeric IP ACL. Input number in ACL number(1-99); set other attributes, and then click Add.



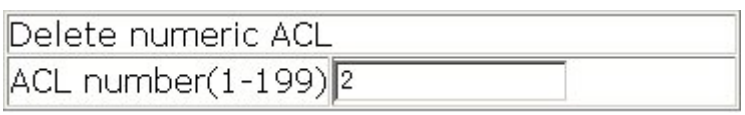
9.5.2Delete standard numeric IP ACL configuration

Click Numeric ACL configuration, Delete numeric ACL rule. The configuration page is shown. See the equivalent CLI command at 9.2.2.1 and 9.2.2.2:

The explanation of each field is as below:

ACL number – ACL number (1-199)

For example: Delete a numeric IP ACL. Input the number of the ACL, and then click Remove.



9.5.3Extended numeric ACL configuration

Users can configure the following types of numeric ACL:
Add ICMP numeric extended ACL - Add ICMP numeric extended ACL
Add IGMP numeric extended ACL - Add IGMP numeric extended ACL
Add TCP numeric extended ACL - Add TCP numeric extended ACL
Add UDP numeric extended ACL - Add UDP numeric extended ACL
Add numeric extended ACL for other protocols - numeric extended ACL for other protocols
Click the node. The configuration page is shown. See the equivalent CLI command at 9.2.2.1

The explanation of each field is as below:
ACL number - ACL number (100-199)
Rule – permit; deny
Source address type – Configure source address type: Specify source address or set to any source address
Source IP address – Specify source IP address
Reverse network mask – Specify reverse network mask
Target address type – Specify target address type: Specify destination address or set to any destination address
Destination IP address – Specify destination IP address
Reverse network mask - Specify reverse network mask
Ip precedence – Specify IP precedence
TOS – Specify TOS value
Operation type – Add; Remove

For ICMP type, the following fields need to be configured:
ICMP type – Specify ICMP type
ICMP code - Specify ICMP code

For IGMP type, the following field needs to be configured:
IGMP type - Specify IGMP type

For TCP type, the following fields need to be configured:
Source port – Specify source port
Target port – Specify the target port
TCP sign – Specify TCP sign

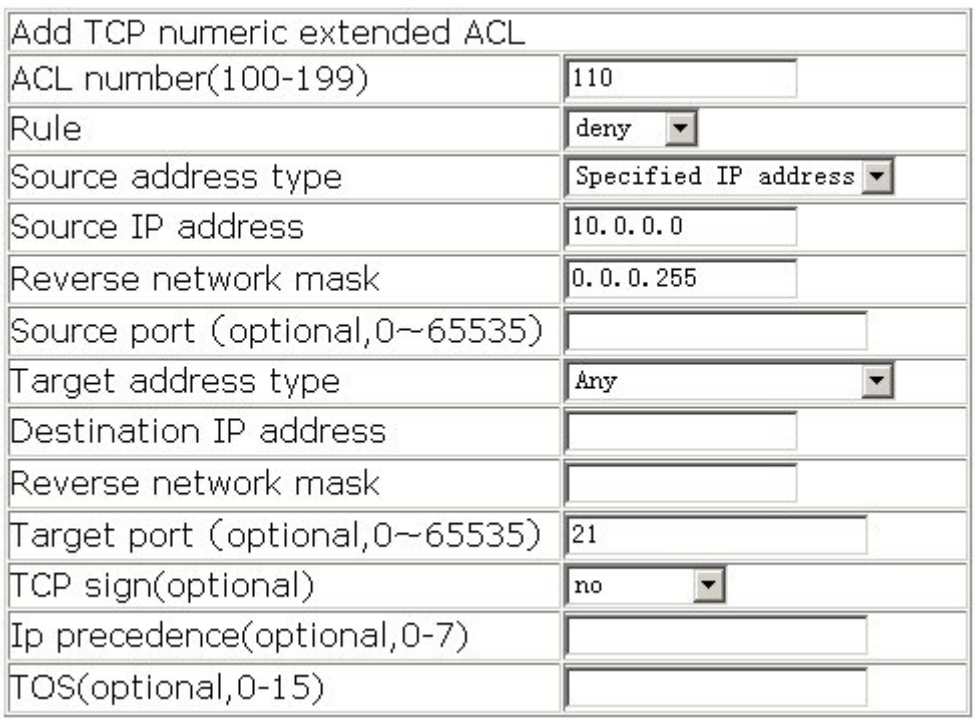
For UDP type, the following fields need to be configured:
Source port – Specify source port

Target port – Specify the target port

For other protocols, the following fields need to be configured:

Matched protocol – Specify the matched protocol: IP, EIGRP, OSPF, IPINIP and Input protocol manually. When “Input protocol manually, users can imput protocol number.

For example: Configure an extended ACL numbered 110 which denies the TCP packets with the source address as 10.0.0.0/24 and target port as 21. Set ACL number (100-199) to 110; set Rule to deny; set Source address type to Specified IP address; set Source IP address to IP10.0.0.0; set Reverse network mask to 0.0.0.255; set Target address type to Any; set Target port to 21, and then click Add.



9.5.4Standard ACL name configuration

Click ACL name configuration. Standard ACL name configuration page is shown. The configuration is very similar to standard numeric ALC configuration, but ACL number field is replaced by ACL name field. See the equivalent CLI command at 9.2.2.6

The explanation of each field is as below:

ACL name – Specify ACL name

ACL type – Specify ACL type: standard and extended

Rule – permi or deny

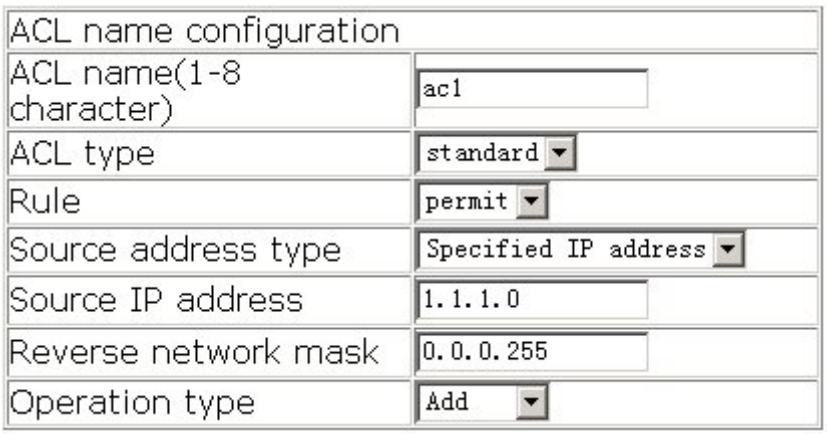
Source address type - Specified IP address or allow any address

Source IP address – Specify source IP address

Reverse network mask – Specify reverse network mask

Operation type – Add; Remove

For example: Add a stanard name ACL. Set ACL name to ac1; configure other fields; set Operation type to Add, and then click Apply.



9.5.5Extended ACL name configuration

Click ACL name configuration. The configuration page is shown:

IP extended ACL name configuration

ICMP extended ACL name configuration

IGMP extended ACL name configuration

TCP extended ACL name configuration

UDP extended ACL name configuration

Other protocols extended ACL name configuration

Click the node. The configuration page is shown. The configuration is very similar to extended numeric ALC configuration, but ACL number field is replaced by ACL name field. See the equivalent CLI command at 9.2.2.5

9.5.6Firewall configuration

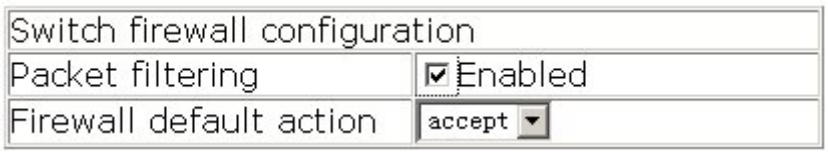
Click Filter configuration. The configuration page is shown.

The explanation of each field is as below:

Packet filtering – Enable or disable. See the equivalent CLI command at 9.2.2.3

Firewall default action – Configure firewall default action. “accept” is used to allow packets to pass; “refuse” is used to deny packets to pass. See the equivalent CLI command at 9.2.2.4

For example: Set Packet filtering to Enable; set Firewall default action to accept, and then click Apply.



9.5.7ACL port binding configuration

Click Filter configuration. The configuration page is shown.. See the equivalent CLI command at 9.2.2.7

The explanation of each field is as below:

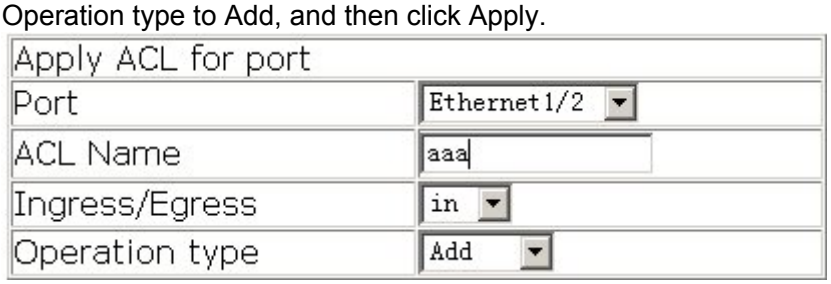
Port – Configure binding port

ACL name – Configure binding ACL nameL

Ingress/Egress – Configure binding direction: Ingress/Egress

Operation type – Add; Remove

For example: Set Port to Ethernet 1/2; set ACL Name to aaa; set Ingress/Egress to in; set Operation type to Add, and then click Apply.



Chapter 10 Port Channel Configuration

10.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first: Port Group is a group of physical ports in the configuration level, only physical ports in the Port Group can take part in link aggregation and become a member port of Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) of the same properties to a logical port. Port Channel is a collection of physical ports and used as one physical port logically. Port Channel can be used as a normal port by the user, and can not only add network bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

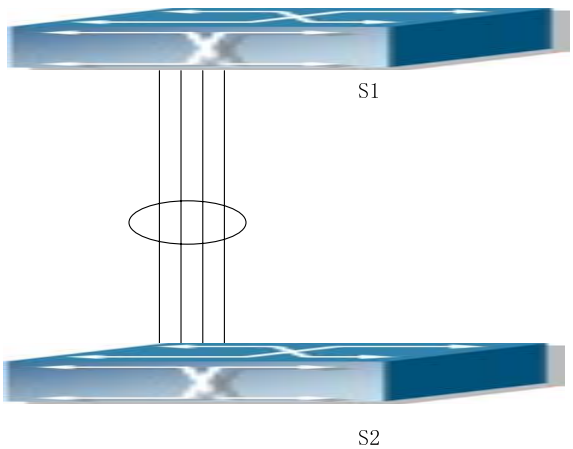


Fig 10-1 Port aggregation

As shown in the above figure, port 1-4 of switch S1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from S1 needs to be transferred to S2 through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address, and the calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through traffic allocation algorithm. Traffic allocation algorithm is determined by the hardware.
ES4626/ES4650 offers 2 methods for configuring port aggregation: manual Port Channel creation, and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as the following:

- ☞ All ports in full duplex mode.
- ☞ Ports are of the same speed.
- ☞ All ports are Access ports and belong to the same VLAN or are all Trunk ports.
- ☞ If the ports are Trunk ports, then their “Allowed VLAN” and “Native VLAN” property should also be the same.

If Port Channel is configured manually or dynamically on ES4626/ES4650, the system will automatically set the port of the smallest number to be Master Port of Port Channel. If spanning tree is enabled in the switch, spanning tree protocol will regard Port Channel as a logical port and sent BPDU frames via the master port.

Port aggregation is closely related with the switch hardware. ES4626/ES4650 series allow physical port aggregation of any two switches, maximum 8 port groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. ES4626/ES4650 has built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical port configuration mode.

10.2 Port Channel Configuration

10.2.1 Port Channel Configuration Task Sequence

1. Create a port group in Global Mode.
2. Add ports to the specified group from the Port Mode of respective ports.
3. Enter port-channel configuration mode.

1. Creating a port group

Command	Explanation
Global Mode	
port-group <*port-group-number*> [load-balance { src-mac | dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}] **no port-group <*port-group-number* > [load-balance]**	Create or delete a port group and set the load balance method for that group.

2. Add physical ports to the port group

Command	Explanation
Interface Mode	
port-group <*port-group-number*> mode {active|passive|on} **no port-group <*port-group-number*>**	Add ports to the port group and set their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel <*port-channel-number*>	Create and enter port-channel configuration mode.

10.2.2 Port Channel Configuration Commands

10.2.2.1 port-group

Command: port-group <*port-group-number*> [load-balance { src-mac|dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}]

no port-group <*port-group-number*> [load-balance]

Function: Create a port group and set the load balance method for that group. If no method is specified, the default load balance method is used. The "**no port-group <*port-group-number*> [load-balance]**" command deletes that group or restores the default load balance setting. Enter "load-balance" for restoring default load balance, otherwise, the group will be deleted.

Parameter: <*port-group-number*> is the group number of a port channel from 1 to 8, if the group number already exists; an error message will be given. **dst-mac** performs load balance according to destination MAC; **src-mac** performs load balance according to source MAC; **dst-src-mac** performs load balance according to source and destination MAC; **dst-ip** performs load balance according to destination IP; **src-ip** performs load balance according to source IP; **dst-src-ip** performs load balance according to destination and source IP. If a port group has formed a port-channel, load balance setting cannot be modified, please set load balance mode before port-channel.

Default: Switch ports do not belong to port channel by default; LACP not enabled by default.

Command mode: Global Mode

Example: Create a port group and set the default load balance method.

Switch(Config)# port-group 1

Delete a port group.

Switch(Config)#no port-group 1

10.2.2.2 port-group mode

Command: port-group <*port-group-number*> mode {active|passive|on}

no port-group <*port-group-number*>

Function: Add the physical port to the port channel; The command "**no port-group <*port-group-number*>**" removes the port from the port channel.

Parameter: <*port-group-number*> sets the port channel number. The valid range is from 1 to 8; **active(0)** enables the LACP on the port and sets it as active mode; **passive(1)** enables the LACP on the port and sets it as passive mode; **on(2)** forces the port to join the port channel and disables the LACP on the port.

Command mode: Interface Mode

Default: By default, no ports belong to any port channels and LACP is not enabled.

Usage Guide: If the port group doesn't exist when joining the port into this port group, this port group is created automatically and the port is joined to the group afterwards. All the ports in a port group have the same mode which is that of the first port of the port group. The ports which have the port mode as on are imperative. That means the port trunking doesn't rely on the port information. As soon as there are more than 2 port in the port group. And the VLAN information of these ports are the same. The port trunking can be established. The ports which join the port group in the active or passive mode run the LACP. One end of the trunking has to be in the active mode for establishment of the trunking. If two ends of the trunking are in the passive mode, the trunking can't be established.

Example: In the interface mode, add the current Ethernet port 1/1 to port group 1 and set the port mode as active.

Switch (Config-Ethernet1/1)#port-group 1 mode active

10.2.2.3 interface port-channel

Command: interface port-channel <*port-channel-number*>

Function: Create and enter the port channel configuration mode

Command mode: Global Mode

Usage Guide: On entering aggregated port mode, configuration to GVRP or spanning tree modules will apply to aggregated ports; if the aggregated port does not exist (i.e. ports have not aggregated), an error message will be displayed and configuration will be

saved and will be restored until the ports are aggregated. Note such restoration will be performed only once, if an aggregated group is ungrouped and aggregated again, the initial user configuration will not be restored. If it is the configuration to other modules, such as shutdown or speed configuration, then the configuration to current port will apply to all member ports in the corresponding port group.

Example: Enter configuration mode for port-channel1.

Switch(Config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

10.3 Port Channel Example

Scenario 1: Configuring Port Channel in LACP.

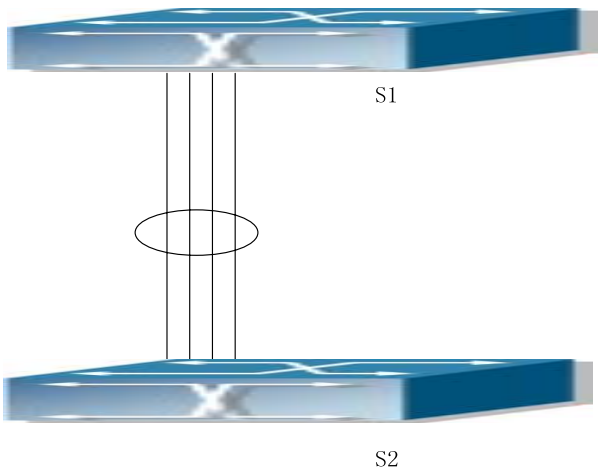


Fig 10-2 Configuring Port Channel in LACP

The switches in the description below are all ES4626/ES4650 switches.

As shown in the figure, port 1, 2, 3 of Switch1 are access ports that belong to vlan1, add those three port to group1 in active mode; port 6, 8, 9 of Switch2 are trunk ports that allow all, add those three ports to group2 in passive mode. All the ports are connected with cables. (the four connecting lines in the figure)

The configuration steps are listed below:

Switch1#config

Switch1 (Config)#interface eth 1/1-3

Switch1 (Config-Port-Range)#port-group 1 mode active

Switch1 (Config-Port-Range)#exit

Switch1 (Config)#interface port-channel 1

Switch1 (Config-If-Port-Channel1)#

Switch2#config

Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 1/6
Switch2 (Config-Ethernet1/6)#port-group 2 mode passive
Switch2 (Config-Ethernet1/6)#exit
Switch2 (Config)# interface eth 1/8-9
Switch2 (Config-Port-Range)#port-group 2 mode passive
Switch2 (Config-Port-Range)#exit
Switch2 (Config)#interface port-channel 2
Switch2 (Config-If-Port-Channel2)#
Configuration result:
Shell prompts ports aggregated successfully after a while, now port 1, 2, 3 of Switch1 forms a aggregated port named “Port-Channel1”, port 6, 8, 9 of Switch2 forms an aggregated port named “Port-Channel2”; configurations can be made in their respective aggregated port configuration mode.

Scenario 2: Configuring Port Channel in ON mode.

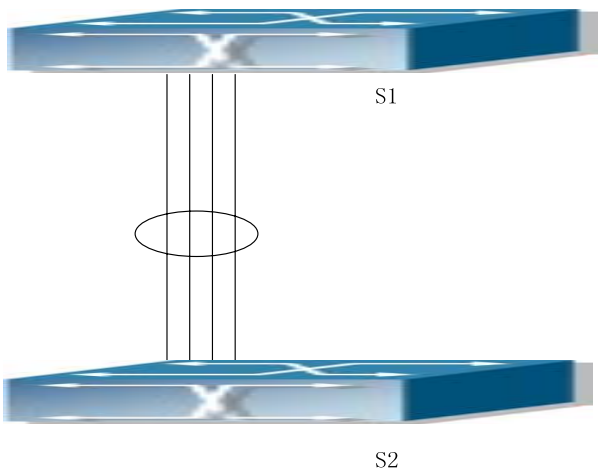


Fig 10-3 Configuring Port Channel in ON mode

As shown in the figure, port 1, 2, 3 of Switch1 are access ports that belong to vlan1, add those three port to group1 in “on” mode; port 6, 8, 9 of Switch2 are trunk port that allow all, add the those three port to group2 in “on” mode.

The configuration steps are listed below:
Switch1#config
Switch1 (Config)#interface eth 1/1
Switch1 (Config-Ethernet1/1)# port-group 1 mode on
Switch1 (Config-Ethernet1/1)#exit
Switch1 (Config)#interface eth 1/2
Switch1 (Config-Ethernet1/2)# port-group 1 mode on

Switch1 (Config-Ethernet1/2)#exit
Switch1 (Config)#interface eth 1/3
Switch1 (Config-Ethernet1/3)# port-group 1 mode on
Switch1 (Config-Ethernet1/3)#exit

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 1/6
Switch2 (Config-Ethernet1/6)#port-group 2 mode on
Switch2 (Config-Ethernet1/6)#exit
Switch2 (Config)# interface eth 1/8-9
Switch2 (Config-Port-Range)#port-group 2 mode on
Switch2 (Config-Port-Range)#exit

Configuration result:
Add port 1, 2, 3 of Switch1 to port-group1 in order, and we can see joining a group in “on” mode is completely forced action, switch in other ends won’t exchange LACP PDU to complete aggregation. Aggregation finishes immediately when command adding port 2 to port-group1 is entered, port 1 and port 2 aggregates to be port-channel1, when port 3 joins port-group1, port-channel1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel1. (it should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregate to form a new group. Now all three ports in both Switch1 and Switch2 are aggregated in “on” mode and become an aggregated port respectively.

10.4 Port Channel Troubleshooting Help

10.4.1 Monitor and Debug Commands

10.4.1.1 show port-group

Command: show port-group [<*port-group-number*>] {brief | detail | load-balance | port | port-channel}
Parameter: <*port-group-number*> is the group number of port channel to be displayed, from 1 to 8; “brief” displays summary information; “detail” displays detailed information; “load-balance ” displays load balance information; “port” displays member port information;

“port-channel” displays port aggregation information.

Command mode: Admin Mode

Usage Guide: If “port-group-number” is not specified, then information for all port groups will be displayed.

Example: Add port 1/1 and 1/2 to port-group1.

1. Display summary information for port-group1.

Switch#show port-group 1 brief

Port-group number : 1

Number of ports in porg-group : 2 Maxports in port-channel = 8

Number of port-channels : 0 Max port-channels : 1

Displayed information	Explanation
Number of ports in group	Port number in the port group
Maxports	Maximum number of ports allowed in a group
Number of port-channels	Whether aggregated to port channel or not
Max port-channels	Maximum port channel number can be formed by port group.

2. Display detailed information for port-group 1.

Switch# show port-group 1 detail

Sorted by the ports in the group 1:

---

port Ethernet1/1 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 1 actor_port_agg_id: 0 partner_oper_sys: 0x000000000000

partner_oper_key: 0x0001 actor_oper_port_key: 0x0101

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: FALSE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as the follow

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

port Ethernet1/2 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 2 actor_port_agg_id: 0 partner_oper_sys: 0x000000000000

partner_oper_key: 0x0002 actor_oper_port_key: 0x0102

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: TRUE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as follows:

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

Displayed information	Explanation
portnumber	Port number
actor_port_agg_id	Number of the channel to add the port. If the port cannot be added to the channel due to inconsistent parameter between the port and the channel, 3 will be displayed,.
partner_oper_sys	System ID of the other end.
partner_oper_key	Operational key of the other end.
actor_oper_port_key	Local end operational key
mode of the port	The mode in which port is added to the group
mac_type	Port type: standard Ethernet port and fiber-optical distributed data interface
speed_type	Port speed type: 10M, 100M, 1,000M and 10G.
duplex_type	Port duplex mode: full duplex and half duplex
port_type	Port VLAN property: access port or trunk port
mux_state	Status of port binding status machine
rcvm_state	Status of port receiving status machine
prm_state	Status of port sending status machine

3. Display load balance information for port-group1.

Switch# show port-group 1 load-balance

The loadbalance of the group 1 based on src MAC address.

4. Display member port information for port-group1.

```
Switch# show port-group 1 port
Sorted by the ports in the group 1 :
-----------------------------------------
the portnum is 1
port Ethernet1/1 related information:

  Actor part
                        Administrative          Operational
  port number                 1
  port priority             0x8000
  aggregator id               0
  port key                  0x0100                0x0101
  port state
  LACP activety               .                     1
  LACP timeout                .                     .
  Aggregation                 1                     1
  Synchronization             .                     .
  Collecting                  .                     .
  Distributing                .                     .
  Defaulted                   1                     1
  Expired                     .                     .

  Partner part
                        Administrative          Operational
  system                  000000-000000         000000-000000
  system priority           0x8000                0x8000
  key                       0x0001                0x0001
  port number                 1                     1
  port priority             0x8000                0x8000
  port state
  LACP activety               .                     .
  LACP timeout                1                     1
  Aggregation                 1                     1
  Synchronization             .                     .
  Collecting                  .                     .
  Distributing                .                     .
  Defaulted                   1                     1
```

Expired . .

Selected Unselected

Displayed information	Explanation
portnumber	Port number
port priority	Port Priority
system	system ID
system priority	System Priority
LACP activety	Whether port is added to the group in “active” mode, 1 for yes.
LACP timeout	Port timeout mode, 1 for short timeout.
Aggregation	Whether aggregation is possible for the port, 0 for independent port that do not allow aggregation.
Synchronization	Whether port is synchronized with the partner end.
Collecting	Whether status of port bound status machine is “collecting” or not.
Distributing	Whether status of port bound status machine is “distributing” or not.
Defaulted	Whether the local port is using default partner end parameter.
Expired	Whether status of port receiving status machine is “expire” or not.
Selected	Whether the port is selected or not..

5. Display port-channel information for port-group1.

Switch# show port-group 1 port-channel

Port channels in the group 1:

Port-Channel: port-channel1

Number of port : 2 Standby port : NULL

Port in the port-channel :

Index Port Mode

---

1 Ethernet1/1 active

2 Ethernet1/2 active

Displayed information	Explanation
Port channels in the group	If port-channel does not exist, the above information would not be displayed.

Number of port	Port number in the port-channel.
Standby port	Port that is in “standby” status, which means the port is qualified to join the channel but cannot join the channel due to the maximum port limit, thus the port status is “standby” instead of “selected”.

10.4.1.2 debug lacp

Command: debug lacp
no debug lacp

Function: Enables the LACP debug function: the “**no debug lacp”** command disables this debug function**.**

Command mode: Admin Mode

Default: LACP debug information is disabled by default.

Usage Guide: Use this command to enable LACP debug so that LACP packet processing information can be displayed.

Example: Enable LACP debug.

Switch#debug lacp

10.4.2 Port Channel Troubleshooting Help

If problems occur when configuring port aggregation, please first check the following for causes.

☞ Ensure all ports in a port group have the same properties, i.e. whether they are in full duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make sure to correct.

☞ Some commands cannot be used on port in port-channel, including: arp, bandwidth, ip, ip-forward, etc.

☞ When port-channel is forced, as the aggregation is triggered manually, the port group will stay unaggregated if aggregation fails due to inconsistent VLAN information. Ports must be added to or removed from the group to trigger another aggregation, if VLAN information inconsistency persists, the aggregation will fail again. The aggregation will only succeed when VLAN information is consistent and aggregation triggered due to port addition or removal.

☞ Verify port group is configured in the partner end, and in the same configuration. If the local end is set in manual aggregation or LACP, the same should be done in the partner end; otherwise part aggregation will not work properly. Another thing to note is that if both ends are configured with LACP, then at least one of them should be in ACTIVE mode,

otherwise LACP packet wouldn't be initialed.

☞ LACP cannot be used on port enabled Security and 802.1x, therefore it cannot be enabled if those two protocols are present on the port.

☞ Port Channel Configuration

10.5 Web Management

Click Port Channel configuration. LACP port group configuration node and LACP port configuration node are shown. LACP port group page is used to configure and show goupe; LACP port page is used to configure and show group member ports.

10.5.1 LACP port group configuration

Click LACP port group configuration. The configuration page is shown. See the equivalent CLI command at 10.2.2.1

The explanation of each field is as below:

Group Num - group number

Load balance mode - Load balance mode: src-mac, dst-mac, dst-src-mac, src-ip, dst-ip and dst-src-ip

Operation type - Add port group or Remove port group

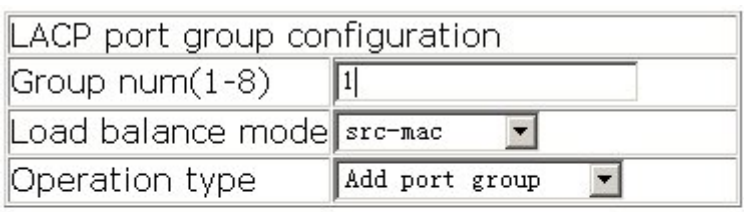
For example: Set group Num to 1; set Load balance mode to src-mac; set Operation type to Add port group, and then click Apply.

After LACP port group is configured, the configuration is shown below.

The explanation of each field is as below:

port group - Port group

load balance - Load balance mode



port group table	
port group	load balance
1	src-mac

10.5.2 LACP port configuration

Click LACP port configuration. The configuration page is shown. See the equivalent CLI command at 10.2.2.2

The explanation of each field is as below:

group num - Group number

Port - Specify the port

Port mode - Configure port mode: active, passive or on

Operation type - Add port to group or Remove port from group

For example: Set group num to 1; set Port to Ethernet 1/1; set Port mode to active; set Operation type to Add port to group, and then click Apply.

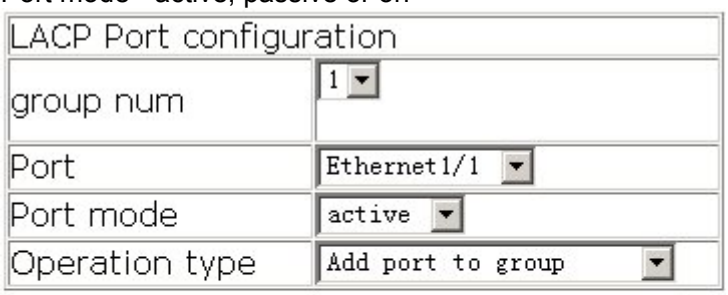
Show member port

After LACP port is configured, the configuration is shown below. See the equivalent CLI command at 10.4.1.1

The explanation of each field is as below:

Port - Member port name

Port mode - active, passive or on



LACP group 1 Port list	
Port	Port mode
Ethernet1/1	active
Ethernet1/2	active

Chapter 11 DHCP Configuration

11.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, default route and host image file position within the network. DHCP is the enhanced version of BootP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of IP allocation and reduce user effort and cost on configuration. Anther benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network, that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server. The implementation of DHCP is shown below:

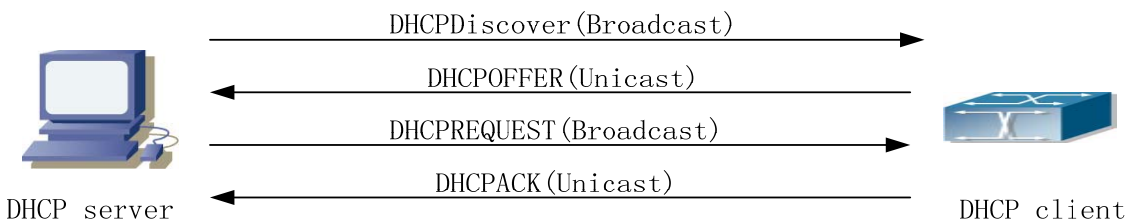


Fig 11-1 DHCP protocol interaction

Explanation:

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.
4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will be sent to the client by the server. In this case, a DHCP relay is required to forward such

DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

ES4626/ES4650 can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are: 1) IP address obtained dynamically can be different every time; manually bound IP address will be the same all the time. 2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless. 3) Dynamically allocated address cannot be bound manually. 4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

11.2 DHCP Server Configuration

11.2.1 DHCP Sever Configuration Task Sequence

2. Enable/Disable DHCP server
3. Configure DHCP Address pool
   (1) Create/Delete DHCP Address pool
   (2) Configure DHCP address pool parameters
   (3) Configure manual DHCP address pool parameters
4. Enable logging for address conflicts

1. Enable/Disable DHCP server

Command	Explanation
Global Mode	
service dhcp **no service dhcp**	Enables DHCP server

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	Explanation
Global Mode	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configures DHCP Address pool

(2) Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Configures the address scope that can be allocated to the address pool
default-router [address1[address2[…address8]]] **no default-router**	Configures default gateway for DHCP clients
dns-server [address1[address2[…address8]]] **no dns-server**	Configures DNS server for DHCP clients
domain-name <*domain*> **no domain-name**	Configures Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [address1[address2[…address8]]] **no netbios-name-server**	Configures the address for WINS server
netbios-node-type {**b-node|h-node|m-node|p-node|<*type-number*>**} **no netbios-node-type**	Configures node type for DHCP clients
bootfile <*filename*> **no bootfile**	Configures the file to be imported for DHCP clients on bootup
next-server [address1[address2[…address8]]] **no next-server [address1[address2[…address8]]]**	Configures the address of the server hosting file for importing
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configures the network parameter specified by the option code
lease { days [hours][minutes] | infinite } **no lease**	Configures the lease period allocated to addresses in the address pool
Global Mode	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Excludes the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specifies the hardware address when assigning address manually
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specifies the IP address to be assigned to the specified client when binding address manually
client-identifier <*unique-identifier*> **no client-identifier**	Specifies the unique ID of the user when binding address manually
client-name <*name*> **no client-name**	Configures a client name when binding address manually

3. Enable logging for address conflicts

Command	Explanation
Global Mode	
ip dhcp conflict logging **no ip dhcp conflict logging**	Enables logging for DHCP address to detect address conflicts
Admin Mode	
clear ip dhcp conflict <*address* | *all*>	Deletes a single address conflict record or all conflict records

11.2.2 DHCP Server Configuration Commands

11.2.2.1 bootfile

Command: bootfile <*filename*>

no bootfile

Function: Set the file name for DHCP client to import on bootup; the "no **bootfile** " command deletes this setting.

Parameter: <*filename*> is the name of the file to be imported, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server

on bootup. This command is together with the “next sever”.

Example: The path and filename for the file to be imported is “c: \temp\nos.img”.
Switch(dhcp-1-config)#bootfile c: \temp\nos.img

Related command: next-server

11.2.2.2 client-identifier

Command: client-identifier <*unique-identifier*>
no client-identifier

Function: Specify the unique ID of the user when binding address manually; the “**no client-identifier**” command deletes the identifier.

Parameter: **<*unique-identifier*>** is the user identifier, in Hex format. Example: 00-00-01-00-00

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with “host” when binding address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in “host” command to the client.

Example: Specify IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: host

11.2.2.3 client-name

Command: client-name <*name*>
no client-name

Function: Specify the username when binding address manually; the “**no client-name**” command deletes the username.

Parameter: **<*name*>** is the name of the user, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Configure a username for the manual binding device, domain should not be included when configuring username.

Example: Set the user with unique id of 00-10-5a-60-af-12 with a username of “network”.

Switch(dhcp-1-config)#client-name network

11.2.2.4 default-router

Command: default-router <address1>[<address2>[…<address8>]]

no default-router

Function: Configure default gateway(s) for DHCP clients; the "**no default-router**" command deletes the default gateway.

Parameter: ***address1…address8*** are IP addresses, in dotted decimal format.

Default: No default gateway is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, Therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Configure default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

11.2.2.5 dns-server

Command: dns-server <address1>[<address2>[…<address8>]]

no dns-server

Function: Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameter: ***address1…address8*** are IP addresses, in dotted decimal format.

Default: No DNS server is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, Therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Set 10.1.128.3 as the DNS server address for DHCP clients.

Switch(dhcp-1-config)#dns-server 10.1.128.3

11.2.2.6 domain-name

Command: domain-name <*domain*>

no domain-name

Function: Configure Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameter: **<*domain*>** is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify a domain name for the client.

Example: Specify “company.com.cn" as the DHCP clients’ domain name.

Switch(dhcp-1-config)#domain-name company.com.cn

11.2.2.7 hardware-address

Command: hardware-address *<hardware-address>* [{Ethernet | IEEE802|*<type-number>*}]

no hardware-address

Function: Specify the hardware address of the user when binding address manually; the “**no hardware-address**” command deletes the setting.

Parameter: *<hardware-address>* is the hardware address in Hex; **Ethernet | IEEE802** is the Ethernet protocol type, ***<type-number>*** should be the number defined in RFC for protocol types, from 1 to 255, e.g. 0 for Ethernet and 6 for IEEE802.

Default: The default protocol type is Ethernet, . .

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with the “host” when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example: Specify IP address 10.1.128.160 to be bound to user with hardware address 00-00-e2-3a-26-04 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: host

11.2.2.8 host

Command: host <address> [<mask> | <prefix-length>]

no host

Function: Specify the IP address to assign to the user when binding address manually; the “**no host**” command deletes the IP address.

Parameter: *<address>* is the IP address in dotted decimal format; ***<mask>*** is the subnet mask in dotted decimal format; ***<prefix-length>*** means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is “24”, and mask 255.255.255.252 in prefix is “30”.

Command Mode: DHCP Address Pool Mode

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the

system will assign a mask automatically according to the IP address class. This command is used with “hardware address” command or “client identifier” command when binding address manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example: Specify IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: hardware-address、client-identifier

11.2.2.9 ip dhcp conflict logging

Command: ip dhcp conflict logging

no ip dhcp conflict logging

Function: Enable logging for address conflicts detected by the DHCP server; the “**no ip dhcp conflict logging”** command disables the logging.

Default: Logging for address conflict is enabled by default.

Command mode: Global Mode

Usage Guide: When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.

Example: Disable logging for DHCP server.

Switch(Config)#no ip dhcp conflict logging

Related command: clear ip dhcp conflict

11.2.2.10 p dhcp excluded-address

Command: ip dhcp excluded-address <*low-address*> [<*high-address*>]

no ip dhcp excluded-address <*low-address*> [<*high-address*>]

Function: Specify addresses excluding from dynamic assignment; the “**no ip dhcp excluded-address <*low-address*> [<*high-address*>]**” command cancels the setting.

Parameter: <*low-address*> is the starting IP address, **[<*high-address*>]** is the ending IP address.

Default: Only individual address is excluded by default.

Command mode: Global Mode

Usage Guide: This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.

Example: Reserve addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.

Switch(Config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

11.2.2.11 ip dhcp pool

Command: ip dhcp pool <*name*>

no ip dhcp pool <*name*>

Function: Configure a DHCP address pool and enter the pool mode; the "**no ip dhcp pool <*name*>"** command deletes the specified address pool.

Parameter: <*name*> is the address pool name, up to 255 characters are allowed.

Command mode: Global Mode

Usage Guide: This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.

Example: Define an address pool named "1".

Switch(Config)#ip dhcp pool 1

Switch(dhcp-1-config)#

11.2.2.12 loghost dhcp

Command: loghost dhcp <*ip-address*> <*port*>

no loghost dhcp

Function: Enable DHCP logging and specify the IP address and port number for the DHCP logging host; the "**no loghost dhcp"** command disables the DHCP logging function.

Parameter: <*ip-address*> is the DHCP log host IP address in dotted decimal format. **<*port*>** is the port number, valid value is 0 – 65535.

Default: DHCP logging is disabled by default.

Command mode: Global Mode

Usage Guide: The user can check information about DHCP address assignment from the log host when this command is configured.

Example: Enable the DHCP logging, the log host is 192.168.1.101, port 45.

Switch(Config)#loghost dhcp 192.168.1.101 45

11.2.2.13 lease

Command: lease { [<*days*>] [<*hours*>][<*minutes*>] | infinite }
no lease

Function: Set the lease for addresses in the address pool; the "**no lease**" command restores the default setting.

Parameter: <*days*> is number of days from 0 to 365; **<*hours*** is number of hours from 0 to 23; **<*minutes*>** is number of miniature from 0 to 59; **infinite** means perpetual use.

Default: The default lease duration is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: DHCP is the protocol to assign network address dynamically instead of permanently, hence the introduction of ease duration. Lease setting should be decided based on the network condition: too long lease duration offsets the flexibility and dynamic of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of ES4626/ES4650 is 1 day.

Example: Set the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

11.2.2.14 netbios-name-server

Command: netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]
no netbios-name-server

Function: Configure WINS servers address; the "**no netbios-name-server**" command deletes the WINS server.

Parameter: *address1…address8* are IP addresses, in the dotted decimal format.

Default: No WINS server is configured by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority, Therefore address1 has the highest priority, and address2 the second, and so on.

11.2.2.15 netbios-node-type

Command: netbios-node-type {**b-node|h-node|m-node|p-node|<*type-number*>**}
no netbios-node-type

Function: Set the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameter: **b-node** stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication; **m-node** for hybrid node communicates in point-to-point after broadcast; **p-node** for point-to-point node; ***<type-number>*** is the node type in Hex from 0 to FF.

Default: No client node type is specified by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example: Set the node type for client of pool 1 to broadcasting node.

Switch(dhcp-1-config)#netbios-node-type b-node

11.2.2.16 network-address

Command: network-address <network-number> [<mask> | <prefix-length>]

no network-address

Function: Set the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameter: ***<network-number>*** is the network number; ***<mask>*** is the subnet mask in the dotted decimal format; ***<prefix-length>*** stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default: If no mask is specified, default mask will be assigned according to the address class.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command "hardware address" and "host".

Example: Configure the assignable address in pool 1 to be 10.1.128.0/24.

Switch(dhcp-1-config)#network-address 10.1.128.0 24

Related command: ip dhcp excluded-address

11.2.2.17 next-server

Command: next-server <address1>[<address2>[…<address8>]]

no next-server

Function: Set the server address for storing the client import file; the "**no next-server**" command cancels the setting.

Parameter: ***address1…address8*** are IP addresses, in the dotted decimal format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration file from the server on bootup. This command is used together with the "bootfile".

Example: Set the hosting server address as 10.1.128.4.

Switch(dhcp-1-config)#next-server 10.1.128.4

Related command: bootfile

11.2.2.18 option

Command: option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function: Set the network parameter specified by the option code; the "**no option <*code*>**" command cancels the setting for option.

Parameter: <*code*> is the code for network parameters; **<*string*>** is the ASCII string up to 255 characters; ***<hex>*** is a value in Hex that no greater than 510 and must be of even length; **<*ipaddress*>** is the IP address in dotted decimal format, up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode

Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example: Set the WWW server address as 10.1.128.240.

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

11.2.2.19 service dhcp

Command: service dhcp

no service dhcp

Function: Enable DHCP server; the "**no service dhcp**" command disables the DHCP service.

Default: DHCP service is disabled by default.

Command mode: Global Mode

Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP service enables, both DHCP server and DHCP relay are enabled. ES4626/ES4650 can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enable DHCP server.

Switch(Config)#service dhcp

11.3 DHCP Relay Configuration

When the DHCP client and server are in different segments, DHCP relay is required to transfer DHCP packets. Adding a DHCP relay makes it unnecessary to configure a DHCP server for each segment, one DHCP server can provide the network configuration parameter for clients from multiple segments, which is not only cost-effective but also management-effective.

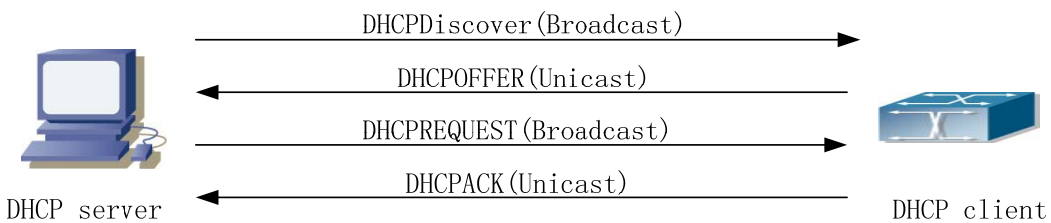


Fig 11-2 DHCP relay

As shown in the above figure, the DHCP client and the DHCP server are in different networks, the DHCP client performs the four DHCP steps as usual yet DHCP relay is added to the process.

1. The client broadcasts a DHCPDISCOVER packet, and DHCP relay inserts its own IP address to the relay agent field in the DHCPDISCOVER packet on receiving the packet, and forwards the packet to the specified DHCP server (for DHCP frame format, please refer to RFC2131).
2. On the receiving the DHCPDISCOVER packets forwarded by DHCP relay, the DHCP server sends the DHCPOFFER packet via DHCP relay to the DHCP client.
3. DHCP client chooses a DHCP server and broadcasts a DHCPREPLY packet, DHCP relay forwards the packet to the DHCP server after processing.
4. On receiving DHCPREPLY, the DHCP server responds with a DHCPACK packet via DHCP relay to the DHCP client.

DHCP relay can not only send DHCP broadcasting packets to the specified DHCP servers, but can also send other specified UDP broadcast packet to specified servers.

11.3.1 DHCP Relay Configuration Task Sequence

1. Enable DHCP relay.
2. Configure DHCP relay to forward DHCP broadcast packet.
3. Configure DHCP relay to forward other UDP broadcast packet.
4. Disable DHCP relay from forwarding DHCP broadcast packet.

1. Enable DHCP relay.

DHCP server and DHCP relay is enabled as the DHCP service is enabled..

2. Configure DHCP relay to forward DHCP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	The UDP port 67 is used for DHCP broadcast packet forwarding.
Interface Mode	
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	Set the destination IP address for DHCP relay forwarding; the "**no ip helper-address <*ipaddress*>**" command cancels the setting.

3. Configure DHCP relay to forward other UDP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	Specify the DHCP relay forwarding protocol by setting UDP port; the "**no ip forward-protocol udp <*port*>**" command cancels the setting.
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	Set the destination IP address for DHCP relay forwarding; the "**no ip helper-address <*ipaddress*>**" command cancels the setting.

4. Disable DHCP relay from forwarding DHCP broadcast packet.

Command	Explanation
Global Mode	
ip dhcp relay information policy drop **no ip dhcp relay information policy drop**	When layer 3 switches are used as DHCP relays, this command sets the relay forwarding policy to drop DHCP packets; the "**no ip dhcp relay information policy drop**" command allows DHCP packets forwarding.

11.3.2 DHCP Relay Configuration Command

11.3.2.1 ip forward-protocol udp

Command: ip forward-protocol udp <port>

no ip forward-protocol udp <port>

Function: Set DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp <port>**" command cancels the service.

Default: DHCP relay forwards DHCP broadcast packet by default (UDP port 67).

Command mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command described later.

Example: Set TFTP packets to be forwarded to 192.168.1.5.

Switch(Config)#ip forward-protocol udp 69

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip helper-address 192.168.1.5

11.3.2.2 ip helper-address

Command: ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

Function: Specify the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address <*ip-address*>**" command cancels the setting.

Default: Address for forwarding DHCP broadcast packet is set on DHCP relay by default.

Command mode: Interface Mode

Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e., DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. The default setting of DHCP relay is to forward DHCP packets on UDP port 67 to DHCP server. When this command is run after "**ip forward-protocol udp <*port*>**" command, the forwarding address configured by this command receives the UDP packets from **<*port*>** instead of default DHCP packets. If a different set of UDP forwarding protocol and receiving server address is to be set, the combination of "**ip forward-protocol udp <*port*>**" command and this command should be used for configuration.

11.3.2.3 ip dhcp relay information policy drop

Command: ip dhcp relay information policy drop

no ip dhcp relay information policy drop

Function: When the layer 3 switch serves as the DHCP relay, users can use this

command to stop the DHCP message forwarding. The command "**no ip dhcp relay information policy drop**" restores the DHCP message forwarding.

Default: DHCP relay forwards DHCP broadcasting messages by default.

Command mode: Global Mode

Usage Guide: When DHCP messages shouldn't be forwarded for certain reasons, this command can be used to stop the forwarding.

Example: Disable DHCP broadcasting messages forwarding function.

Switch(Config)# ip dhcp relay information policy drop

11.4 DHCP Configuration Example

Scenario 1:

Too save configuration efforts of network administrators and users, a company is using ES4626/ES4650 as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WINS server	10.16.1.209
WINS node type	H-node	WINS node type	H-node
Lease	3 days	Lease	3 days

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as "management". (The interfaces in the following configurations are wrong; "no switch" command is not available.)

Switch(Config)#service dhcp

Switch(Config)#interface vlan 1

Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0

Switch(Config-Vlan-1)#exit

Switch(Config)#ip dhcp pool A

Switch(dhcp-A-config)#network 10.16.1.0 24

Switch(dhcp-A-config)#lease 3

Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201

Switch(dhcp-A-config)#dns-server 10.16.1.202

Switch(dhcp-A-config)#netbios-name-server 10.16.1.209

Switch(dhcp-A-config)#netbios-node-type H-node

Switch(dhcp-A-config)#exit

Switch(Config)#ip dhcp excluded-address 10.16.1.200 10.16.1.210

Switch(Config)#ip dhcp pool B

Switch(dhcp-B-config)#network 10.16.2.0 24

Switch(dhcp-B-config)#lease 1

Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201

Switch(dhcp-B-config)#dns-server 10.16.2.202

Switch(dhcp-B-config)#option 72 ip 10.16.2.209

Switch(dhcp-config)#exit

Switch(Config)#ip dhcp excluded-address 10.16.2.200 10.16.2.210

Switch(Config)#ip dhcp pool A1

Switch(dhcp-A1-config)#host 10.16.1.210

Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab

Switch(dhcp-A1-config)# client-name management

Switch(dhcp-A1-config)#exit

Scenario 2:

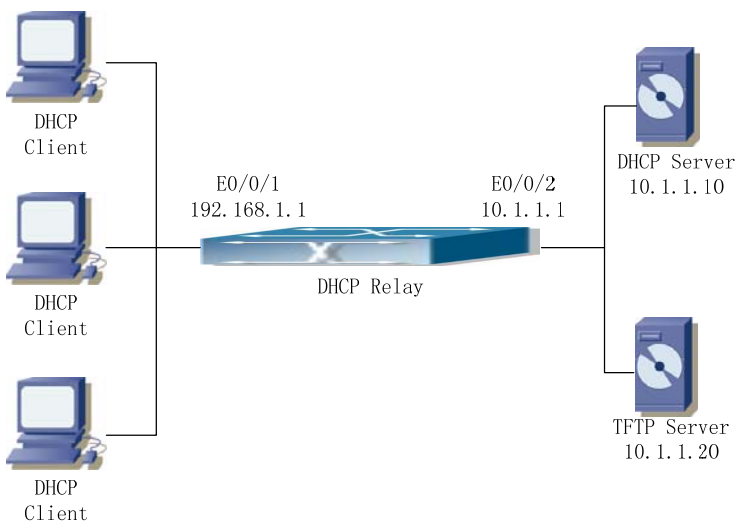


Fig 11-3 DHCP Relay Configuration

As shown in the above figure, route switch is configured as a DHCP relay. The DHCP server address is 10.1.1.10, TFTP server address is 10.1.1.20, the configuration steps is as follows:

Switch (Config)#service dhcp

Switch (Config)#interface vlan 1

Switch (Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0

Switch (Config-if-Vlan1)#exit

```
Switch (Config)#vlan 2
Switch (Config-Vlan-2)#exit
Switch (Config)#interface Ethernet 1/2
Switch (Config-Erthernet1/2)#switchport access vlan 2
Switch (Config-Erthernet1/2)#exit
Switch (Config)#interface vlan 2
Switch (Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch (Config-if-Vlan2)#exit
Switch (Config)#ip forward-protocol udp 67
Switch (Config)#interface vlan 1
Switch (Config-if-Vlan1)#ip help-address 10.1.1.10
Switch (Config-if-Vlan1)#exit
Switch (Config)#ip forward-protocol udp 69
Switch (Config)#interface vlan 1
Switch (Config-if-Vlan1)#ip help-address 10.1.1.20
Switch (Config-if-Vlan1)#exit
```

Note: DHCP server address and TFTP server address must be configured separately since their receiving UDP protocols are different. It is recommended to use the combination of command "**ip forward-protocol udp *<port>***" and "**ip helper-address *<ipaddress>***". "**ip help-address**" can only be configured for ports on layer 3 and cannot be configured on layer 2 ports directly.

Usage Guide:

When a DHCP/BootP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.

If the DHCP/BootP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

11.5 DHCP Troubleshooting Help

11.5.1 Monitor and Debug Commands

11.5.1.1 clear ip dhcp binding

Command: clear ip dhcp binding {<*address*> | all }

Function: Delete the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameter: <*address*> is the IP address that has a binding record, in dotted decimal format. **all** refers to all IP addresses that have a binding record.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.

Example: Remove all IP-hardware address binding records.

Switch#clear ip dhcp binding all

Related command: show ip dhcp binding

11.5.1.2 clear ip dhcp conflict

Command: clear ip dhcp conflict {<*address*> | all }

Function: Delete an address present in the address conflict log.

Parameter: <*address*> is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp conflict**" command can be used to check which IP addresses are conflicting for use, while this command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.

Example: The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.

Switch#clear ip dhcp conflict 10.1.128.160

Related command: ip dhcp conflict logging，show ip dhcp conflict

11.5.1.3 clear ip dhcp server statistics

Command: clear ip dhcp server statistics

Function: Delete the statistics for DHCP server, clear the DHCP server count.

Command mode: Admin Mode

Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use this command to clear the count for easier statistics checking.

Example: clear the count for DHCP server.

Switch#clear ip dhcp server statistics

Related command: show ip dhcp server statistics

11.5.1.4 show ip dhcp binding

Command: show ip dhcp binding [[<*ip-addr*>] + [type {all | manual | dynamic}] [count]]

Function: display IP-MAC binding information.

Parameter: <*ip-addr*> is a specified IP address in dotted decimal format; "all" stands for all binding types (manual binding and dynamic assignment); "manual" for manual binding; "dynamic" for dynamic assignment; "count" displays statistics for DHCP address binding entries.

Command mode: Admin Mode

Example:

Switch# show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment.

11.5.1.5 show ip dhcp conflict

Command: show ip dhcp conflict

Function: Display log information for address that has conflict record.

Command mode: Admin Mode

Example:

Switch# show ip dhcp conflict

IP Address Detection method Detection Time

10.1.1.1 Ping FRI JAN 02 00: 07: 01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

11.5.1.6 show ip dhcp server statistics

Command: show ip dhcp server statistics

Function: Display statistics of all DHCP packets for a DHCP server.

Command mode: Admin Mode

Example:

Switch# show ip dhcp server statistics

Address pools 3

Database agents 0

Automatic bindings 2

Manual bindings 0

Conflict bindings 0

Expired bindings 0

Malformed message 0

Message Received

BOOTREQUEST 3814

DHCPDISCOVER 1899

DHCPREQUEST 6

DHCPDECLINE 0

DHCPRELEASE 1

DHCPINFORM 1

Message	Send
BOOTREPLY	1911
DHCPOFFER	6
DHCPACK	6
DHCPNAK	0
DHCPRELAY	1907
DHCPFORWARD	0

Switch#

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

11.5.1.7 debug ip dhcp server

Command: debug ip dhcp server { events|linkage|packets }

no debug ip dhcp server { events|linkage|packets }

Function: Enable DHCP server debug information: the "**no debug ip dhcp server { events|linkage|packets }"** command disables the debug information for DHCP server**.**

Default: Debug information is disabled by default.

Command mode: Admin Mode

11.5.2 DHCP Troubleshooting Help

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

- ☞ Verify the DHCP server is running, start the related DHCP server if not running.
- ☞ If the DHCP clients and servers are not in the same physical network, verify the router responsible for DHCP packet forwarding has DHCP relay function. If DHCP relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCP relay function.
- ☞ In such case, DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present, (This does not indicate ES4626/ES4650 cannot assign IP address for different segments, see solution 2 for details.)

In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command "**network-address**" and "**host**" are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

11.6 WEB Management

Click DHCP configuration. Users can configure DHCP on the switch.

11.6.1 DHCP server configuration

Click DHCP configuration, DHCP server configuration, The DHCP server configuration page is shown.

11.6.1.1 Enable DHCP

Click DHCP configuration, DHCP server configuration, Enable DHCP. Users can enable or disable DHCP server, and configure logging server:

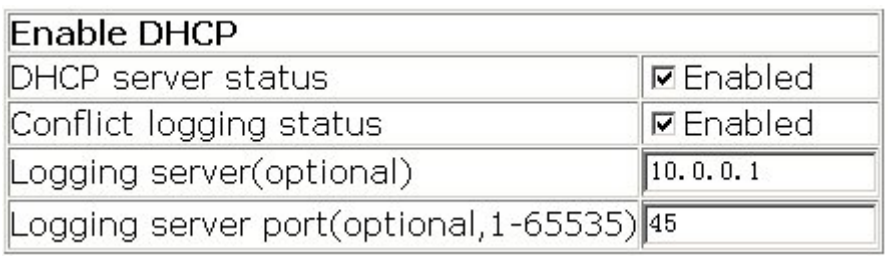
DHCP server status – Enable or disable DHCP server. See the equivalent CLI command at 11.2.2.19

Conflict logging status – Enable or disable conflict logging. See the equivalent CLI command at 11.2.2.9

Logging server(optional) – Specify DHCP logging server IP address. See the equivalent CLI command at 11.2.2.12

Logging server port(optional,1-65535) - Specify DHCP logging server port number

For example: Set DHCP server status to Enabled; set Conflict logging status to Enabled; set Logging server to 10.0.0.1; set Logging server port to 45, and then click Apply. The configuration is applied on the switch.



11.6.1.2 Address pool configuration

Click DHCP configuration, DHCP server configuration, Address pool configuration. Users can configure DHCP address pool:

DHCP pool name (1-32 character) - Configure DHCP pool name. See the equivalent CLI command at 11.2.2.11

DHCP pool domain name(1-255 character) – Configure DHCP client pool domain name. See the equivalent CLI command at 11.2.2.6

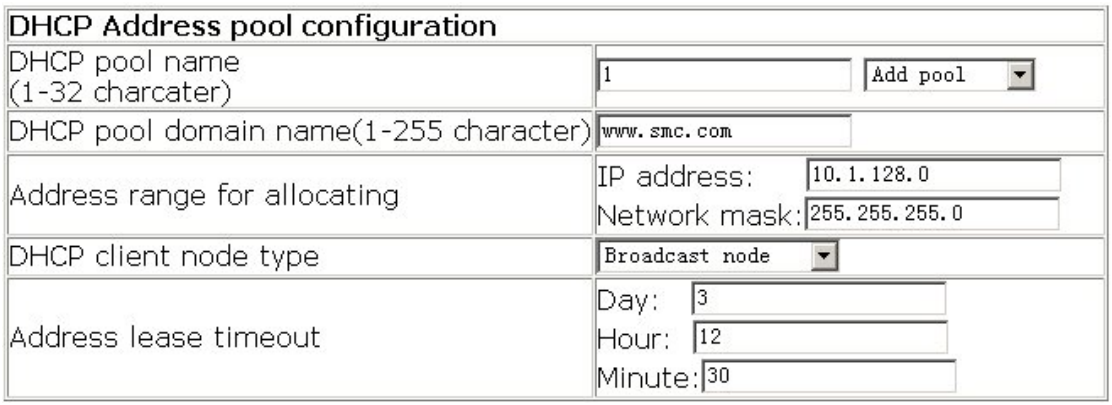
Address range for allocating – Configure address range for allocating. See the equivalent CLI command at 11.2.2.16

DHCP client node type – Configure DHCP client node type: broadcast node; Hybrid node (peer-to-peer -> broadcast); Mixed node (broadcast -> peer-to-peer); Peer-to-peer node. See the equivalent CLI command at 11.2.2.15

Address lease timeout – Configure address lease timeout. See the equivalent CLI command at 11.2.2.13

For example: Set DHCP pool name to 1; set DHCP pool domain name to

www.edge-core.com; for Address range for allocating, set IP address to 10.1.128.0; set Network mask to 255.255.255.0; set DHCP client node type to broadcast node; set Address lease timeout to 3 day 12 hour 30 minute, and then click Apply. The configuration is applied on the switch.



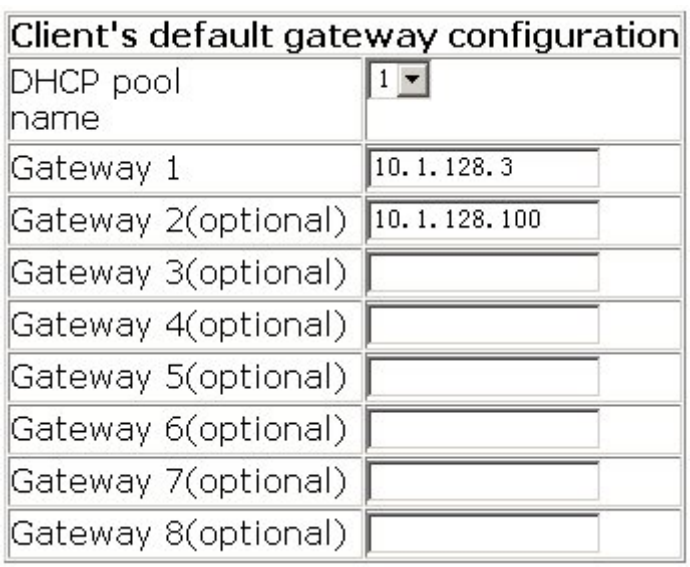
11.6.1.3 Client's default gateway configuration

Click DHCP configuration, DHCP server configuration, Client's default gateway configuration. Users can configure DHCP client's default gateway. See the equivalent CLI command at 11.2.2.4:

DHCP pool name – Select a DHCP pool

Gateway – Configure default gateway. The default gateway IP address should be in the same subnet as DHCP clients. Users can configure maximum eight gateway addresses. Gateway 1 has the highest priority and Gateway 8 has the lowest priority.

For example: Select DHCP pool name to 1; set Gateway 1 to 10.1.128.3; Gateway 2 to 10.1.128.100, and then click Apply. The configuration is applied on the switch.



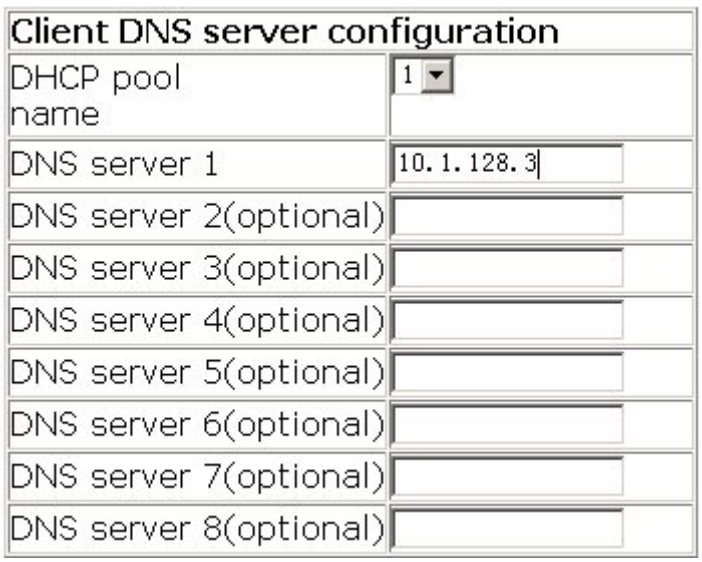
11.6.1.4 Client DNS server configuration

Click DHCP configuration, DHCP server configuration, Client DNS server configuration. Users can configure DHCP client DNS server. See the equivalent CLI command at 11.2.2.5:

DHCP pool name – Select DHCP pool

DNS server - Configure DNS server. Users can configure maximum eight DNS servers. DNS server 1 has the highest priority and DNS server 8 has the lowest priority.

For example: Select DHCP pool name to 1; set DNS server 1 to 10.1.128.3, and then click Apply. The configuration is applied on the switch.



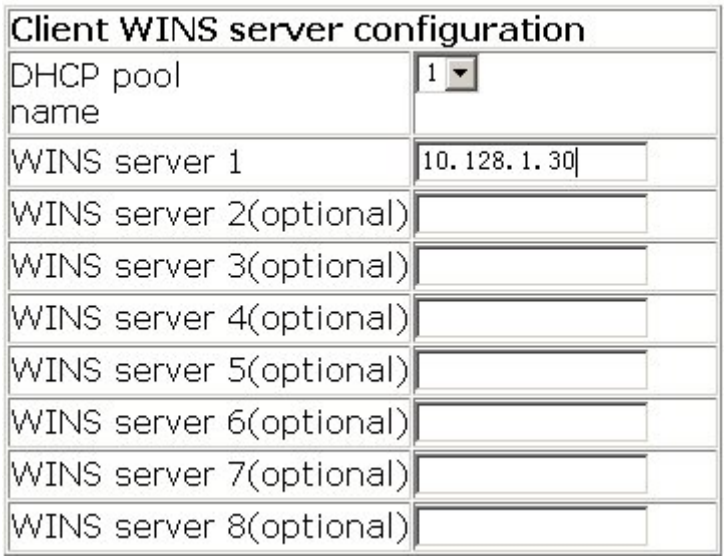
11.6.1.5 Client WINS server configuration

Click DHCP configuration, DHCP server configuration, Client WINS server configuration. Users can configure Wins server. See the equivalent CLI command at 11.2.2.14:

DHCP pool name – Select DHCP pool name

WINS server – Configure WINS server. Users can configure maximum eight WINS server. WINS server 1 has the highest priority and WINS server 8 has the lowest priority.

For example: Select DHCP pool name to 1; set WINS server 1 to 10.1.128.30, and then click Apply. The configuration is applied on the switch.



11.6.1.6 DHCP file server address configuration

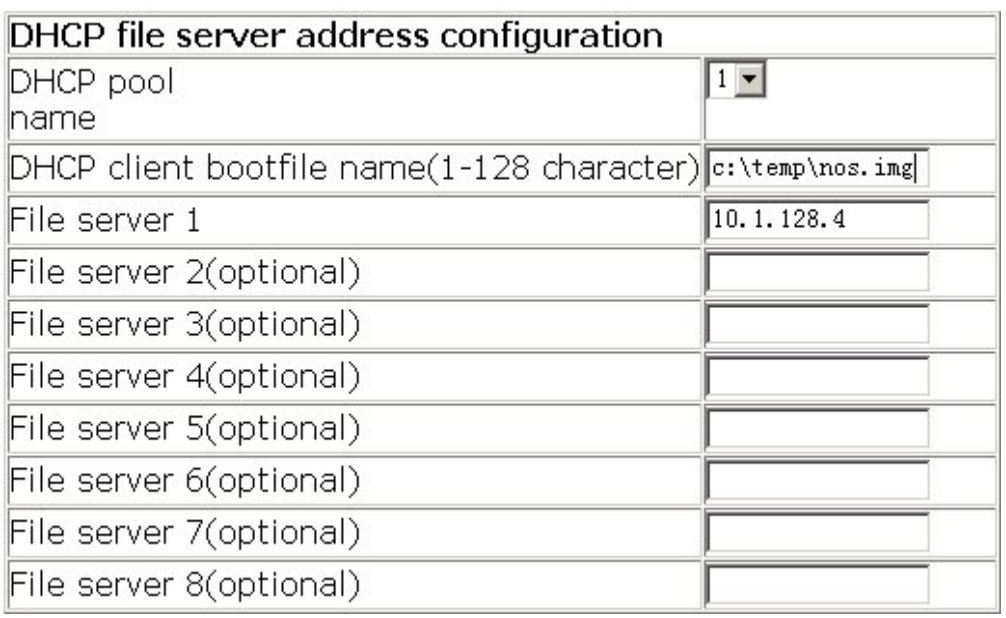
Click DHCP configuration, DHCP server configuration, DHCP file server address configuration. Users can configure DHCP client bootfile name and file server:

DHCP pool name – Select DHCP pool name

DHCP client bootfile name (1-128 character) – Specify bootfile name. See the equivalent CLI command at 11.2.2.1

File server – Specify file server. See the equivalent CLI command at 11.2.2.17

For example: Select DHCP pool name to 1; Set DHCP client bootfile name to c: \temp\nos.img; set File server1 to 10.1.128.4, and then click Apply. The configuration is applied on the switch.



11.6.1.7 DHCP network parameter configuration

Click DHCP configuration, DHCP server configuration, DHCP network parameter configuration. Users can specify DHCP network parameters. See the equivalent CLI command at 11.2.2.18:

DHCP pool name – Select DHCP pool name

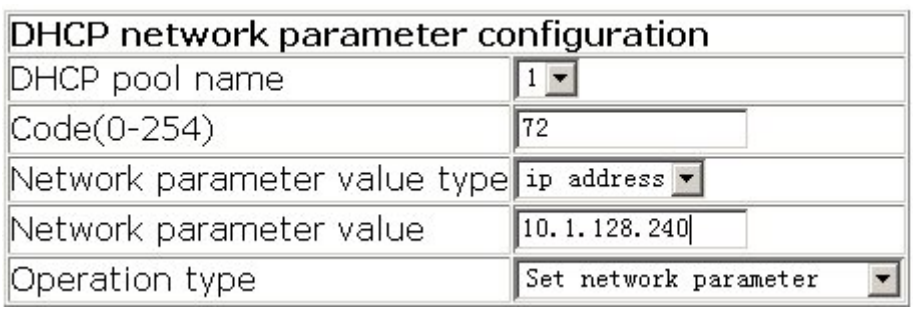
Code(0-254) – Specify network code

Network parameter value type – Configure network parameter value type: ascii, hex or ip address

Network parameter value – Specify network parameter value

Operation type – Apply or cancel the configuration

For example: Select DHCP pool name to 1; set Code to 72; set Network parameter value type to ip address; set Network parameter value to 10.1.128.240; set Operation type to Set network parameter, and then click Apply. The configuration is applied on the switch.



11.6.1.8 Manual address pool configuration

Click DHCP configuration, DHCP server configuration, Manual address pool configuration.Users can configure DHCP manual address pool:

DHCP pool name – Select DHCP pool name

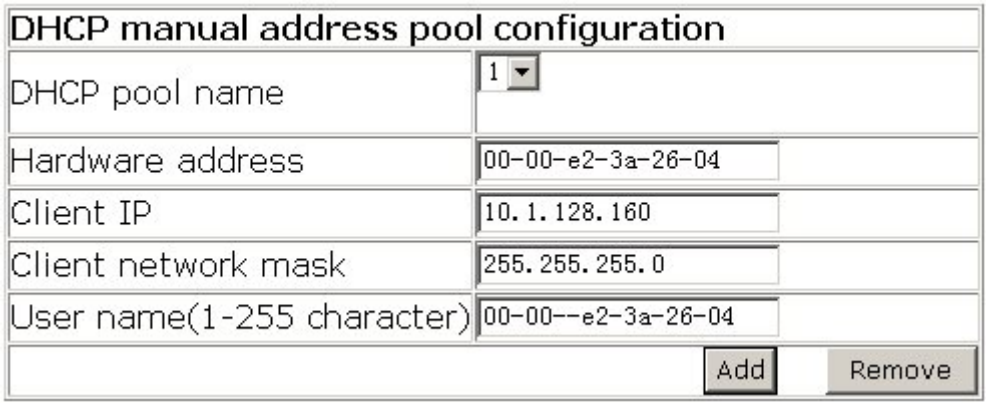
Hardware address – Specify hardware address. See the equivalent CLI command at 11.2.2.7

Client IP – Specify client IP address

Client network mask – Specify client network mask. See the equivalent CLI command at 14.2.2.8

User name(1-255 character) – Specify user name. See the equivalent CLI command at 11.2.2.2

For example: Select DHCP pool name to 1; set Hardware address to 00-00-e2-3a-26-04; set Client IP to 10.1.128.160; set Client network mask to 255.255.255.0; set User name to 00-00-e2-3a-26-04, and then Apply. The configuration is applied on the switch.



11.6.1.9 Excluded address

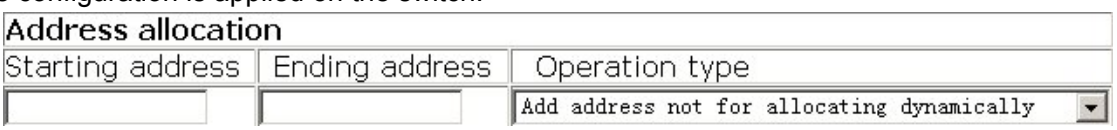
Click DHCP configuration, DHCP server configuration, Manual address pool configuration.Users can configure the exclusive addresses on the DCHP pool. See the equivalent CLI command at 11.2.2.10:

Starting address – Specify starting address

Ending address - Specify ending address

Operation type – Apply or delete the operation

For example: Set Starting address to 10.1.128.1; set Ending address to 10.1.128.10; set Operation type to Add address not for allocating dynamically, and then click Apply. The configuration is applied on the switch.



11.6.1.10 DHCP packet statistics

Click DHCP configuration, DHCP server configuration, DHCP packet statistics. Users can display DHCP packet statistics. See the equivalent CLI command at 11.5.1.3:

DHCP packet statistics	
Memory usage rate	188
Address pool	1
Proxy database	0
Dynamical allocated address	0
Manual binded address	0
Address conflict	0
Binding exceeding lease time	0
Errors	0
Received DHCP packet statistics	
Received	0
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Transmitted DHCP packet statistics	
Transmitted	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0
DHCPRELAY	0

11.6.2 DHCP relay configuration

Click DHCP configuration, DHCP relay configuration. Users can configure DHCP relay.

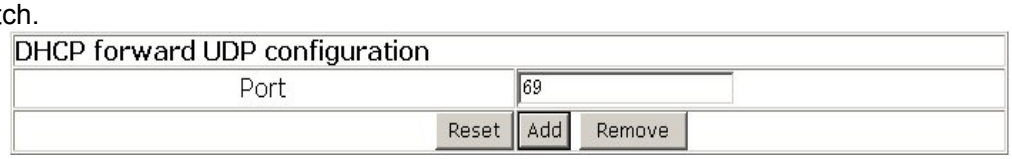
11.6.2.1 DHCP relay configuration

Click DHCP configuration, DHCP relay configuration, DHCP relay configuration. Users can configure DHCP relay:

DHCP forward UDP configuration: Configure DHCP port to forward UDP packets. See the equivalent CLI command at 11.3.2.1:

Port – Specify UDP port

For example: Set Port to 69, and then click Add. The configuration is applied on the switch.



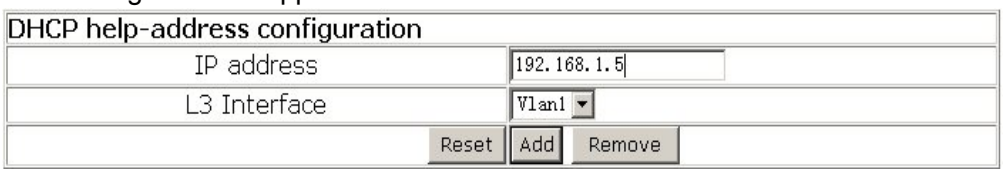
DHCP help-address configuration: Configure DHCP destination address of UDP

packet. See the equivalent CLI command at 11.3.2.2:

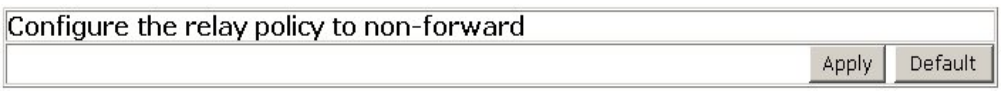
IP address – Specify server IP address

L3 Interface – Specify layer 2 interface

For example: Set IP address to 192.168.1.5; set L3 Interface to Vlan1, and then click Add. The configuration is applied on the switch.



Configure the relay policy to non-forward: Click Apply, DHCP relay is disabled on the switch; click Default, DHCP relay is enabled on the switch.



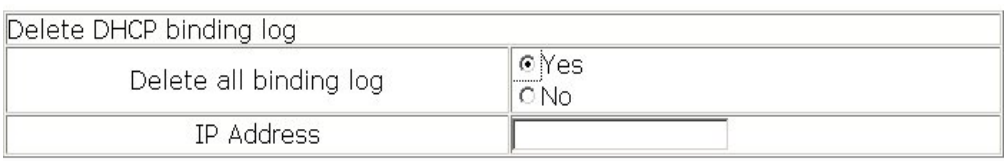
11.6.3 DHCP debugging

Click DHCP configuration, DHCP debugging. Users can display DHCP debug information.

11.6.3.1 Delete binding log

Click DHCP configuration, DHCP debugging, Delete binding log. Users can delete specified binding log or all binding logs.

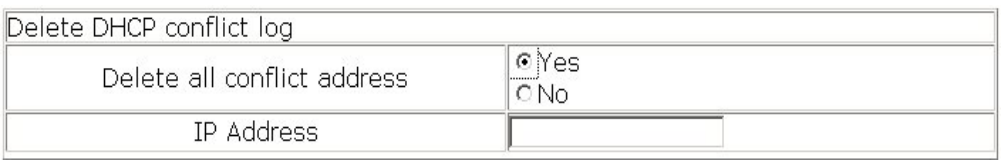
For example: Set Delete all binding log to Yes, and then click Apply. All the binding logs are deleted.



11.6.3.2 Delete conflict log

Click DHCP configuration, DHCP debugging, Delete conflict log. Users can delete conflict log.

For example: Delete all conflict address to Yes, and then click Apply. All the conflict logs are deleted.



11.6.3.3 Delete DHCP server statistics log

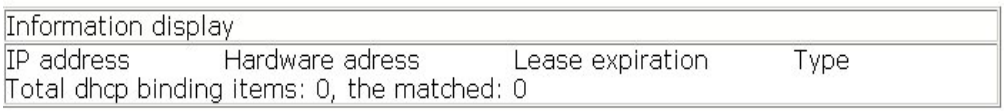
Click DHCP configuration, DHCP debugging, Delete DHCP server statistics log. Users can delete DHCP server statistics and restore the counter to zero.

For example: Click Apply. All the DHCP statistics are deleted.



11.6.3.4 Show IP-MAC binding

Click DHCP configuration, DHCP debugging, Show IP-MAC binding. Users can display IP-MAC binding.



11.6.3.5 Show conflict-logging

Click DHCP configuration, DHCP debugging, Show conflict-logging. Users can display conflict logging.



Chapter 12 SNTP Configuration

The Network Time Protocol (NTP) is widely used for clock synchronization for global computers connected to the Internet. NTP can assess packet sending/receiving delay in the network, and estimate computer clock deviation independently, so as to achieve high accuracy in network computer clocking. In most positions, NTP can provide accuracy from 1 to 50ms according to the characteristics of the synchronization source and network route.

Simple Network Time Protocol (SNTP) is the simplified version of NTP that removed complex algorithm of NTP. SNTP is used for hosts do not require full NTP functions, it is a subset of NTP. It is a common practice to synchronize the clocks of several hosts in local area network with other NTP hosts through the Internet, and use those hosts to provide time synchronization service for other clients in LAN.

ES4626/ES4650 has SNTPv4 client implemented and support SNTP client unicast described in RFC2030; SNTP client multicast and anycast are not supported, nor is SNTP server function.

12.1 SNTP Configuration Commands

12.1.1 sntp server

Command: sntp server <*server_address*> [version <*version_no*>]

no sntp server <*server_address*>

Function: Set the SNTP/NTP server address and server version; the "**no sntp server <*server_address*>**" command deletes the SNTP/NTP server address.

Parameter: <*server-address*> is the IP unicast address of SNTP/NTP server, in dotted decimal format; **<*version_no*>** is the client SNTP version number, valid value is 1 – 4. Default version number is 1.

Default: This setting is not configured upon switch shipment.

Command mode: Global Mode

Example: Set a SNTP/NTP server address.

Switch(Config)#sntp server 10.1.1.1 version 4

12.1.2 sntp poll

Command: sntp poll <*interval*>

no sntp poll

Function: Set the interval for SNTP client to send request to NTP/SNTP; the "**no sntp polltime**" command cancels polltime set and restores the default setting.

Parameter: < *interval*> is the interval value from 16 to 16284.

Default: The default poll is 64 seconds.

Command mode: Global Mode

Example: Set the client to send request to the server every 128 seconds.

Switch#config

Switch(Config)#sntp poll 128

12.1.3 clock timezone

Command: clock timezone <*name*> hour <*hours*> [minute <*minutes*>] [before-utc | after-utc]

Function: Set the time difference between the time zone in which the SNTP client resides and UTC. The "**no sntp timezone**" command cancels the time zone set and restores the default setting.

Parameter: <*name*> is the time zone name, up to 16 characters are allowed;

<before-utc> means the time zone equals UTC time plus **<*hours*> *and* <*munites*>**;

<after-utc> means the time zone equals UTC time minus **<*hours*> *and* <*munites*>**;

<*hours*> *and* <*munites*> are the time difference, range of **<*hours*>*is*** from 1 to 12, range of **<*munites*>**from 0 to 59.

Default: <*munites*> default is 0

Command mode: Global Mode

Example: Set the time zone to Beijing.

Switch#config

Switch(Config)# clock timezone beijing hour 8 before-utc sntp timezone beijing add 8

12.2 Typical SNTP Configuration Examples

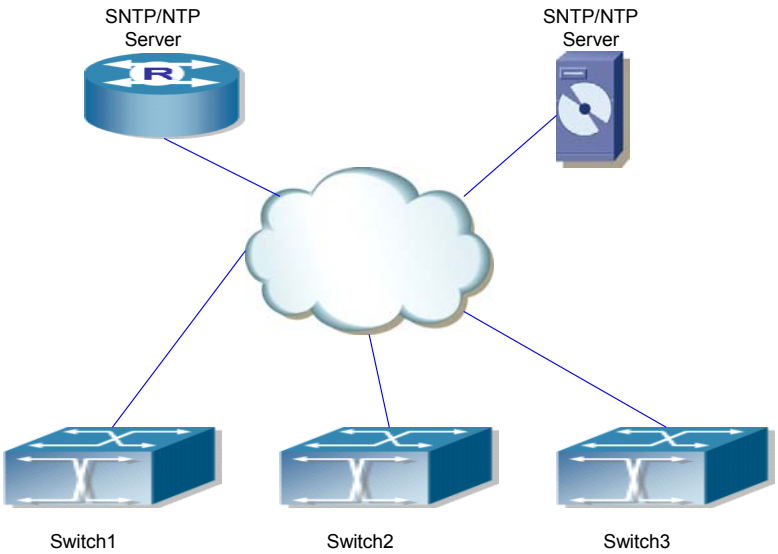


Fig 12-1 Typical SNTP Configuration

All ES4626/ES4650 switches in the autonomous zone are required to perform time synchronization, which is done through two redundant SNTP/NTP servers. For time to be synchronized, the network must be properly configured. There should be reachable route between any ES4626/ES4650 and the two SNTP/NTP servers. Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1, respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any ES4626/ES4650 should like the following:

Switch#config

Switch (Config)#sntp server 10.1.1.1

Switch (Config)#sntp server 20.1.1.1

From now on, SNTP would perform time synchronization to the server according to the default setting (polltime 64s, version 1).

12.3 SNTP Troubleshooting Help

12.3.1 Monitor and Debug Commands

12.3.1.1 show sntp

Command: show sntp

Function: Display current SNTP client configuration and server status.

Parameter: N/A.

Command mode: Admin Mode

Example: Display current SNTP configuration.

Switch#show sntp

SNTP server	Version	Last Receive
2.1.0.2	1	never

12.3.1.2 debug sntp

Command: debug sntp {adjust | packets | select }

no debug sntp {adjust | packets | select}

Function: Display or disable SNTP debug information.

Parameter: adjust stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection.

Command mode: Admin Mode

Example: Display debugging information for SNTP packets.

Switch#debug sntp packets

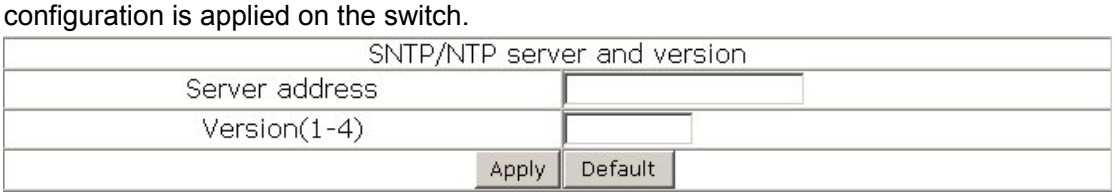
12.4 WEB Management

Click SNTP configuration. Users can configure SNTP on the switch.

12.4.1 12.4.1 SNTP/NTP server configuration

Click SNTP configuration, SNTP/NTP server configuration. Users can configure SNTP/NTP server address and SNTP/NTP version. See the equivalent CLI command at 12.1.1

For example: Set Server address to 12.1.1.1; set version to 4, and then click Apply. The configuration is applied on the switch.



12.4.2 12.4.2 Request interval configuration

Click SNTP configuration, Request interval configuration. Users can configure the

interval of sending request from SNTP client to NTP/SNTP server. See the equivalent CLI command at 12.1.2

For example: Set Interval to 128, and then click Apply. The configuration is applied on the switch.

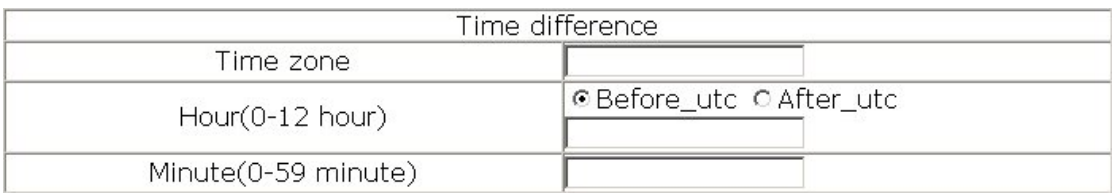


12.4.3 12.4.3 Time difference

Click SNTP configuration, Time difference. Users can configure SNTP client time difference. See the equivalent CLI command at 12.1.3

- Time zone – Configure time zone.
- Time difference – Configure time difference
- Before_utc – Specify the hours added to UTC
- After_utc – Specify the hours which UTC subtracts from.

For example: Set Time zone to Beijing, and then click Add; set Hour to 8, and then click Apply. The configuration is applied on the switch.



12.4.4 12.4.4 Show sntp

Click SNTP configuration, Show sntp. Users can display SNTP client configuration and SNTP server status. See the equivalent CLI command at 12.3.1.1



Chapter 13 QoS Configuration

13.1 QoS

13.1.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

13.1.1.1 QoS Terms

CoS: Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

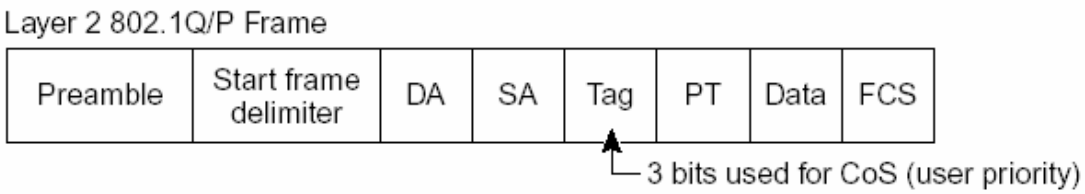


Fig 13-1 CoS priority

ToS: Type of Service, a one byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

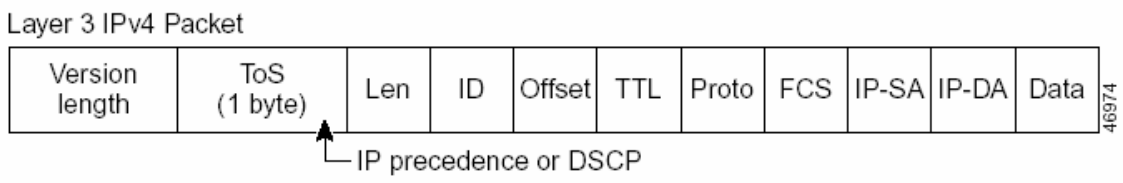


Fig 13-2 ToS priority

IP Precedence: IP priority, classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark: Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Queuing: Egress QoS action, put the packets to appropriate egress queues according to the packet CoS value.

Scheduling: QoS egress action, configure the weight for eight egress queue WRR (Weighted Round Robin).

In Profile: Traffic within the QoS policing policy range (bandwidth or burst value) is called “In Profile".

Out of Profile: Traffic out the QoS policing policy range (bandwidth or burst value) is called “Out of Profile".

13.1.1.2 QoS Implementation

To implement Layer 3 switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and

may discard some low priority packets in case of bandwidth shortage.
If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

13.1.1.3 Basic QoS Model

The basic QoS consists of five parts: Classification, Policing, Remark, Queuing and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.

Classification: Classify traffic according to packet classification information and generate internal DSCP value based on the classification information.

Policing and remark: Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.
Policing can be performed based on DSCP value to configure different policies that allocate bandwidth to classified traffic. If the traffic exceeds the bandwidth set in the policy (out of profile), the out of profile traffic can be allowed, discarded or remarked. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet; this is also called “marking down”.

Queuing and scheduling: Packets at the egress will re-map the internal DSCP value to CoS value, the queuing operation assigns packets to appropriate queues of priority according to the CoS value; while the scheduling operation performs packet forwarding according to the prioritized queue weight.

13.1.2 QoS Configuration

13.1.2.1 QoS Configuration Task Sequence

1. Enable QoS
   QoS can be enabled or disabled in Global Mode. QoS must be enabled first in Global Mode to configure the other QoS commands.
2. Configure class map.
   Set up a classification rule according to ACL, VLAN ID, IP Precedence or DSCP to

classify the data stream. Different classes of data streams will be processed with different policies.

3. Configure a policy map.

   After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading, assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

4. Apply QoS to the ports

   Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

5. Configure queue out method and weight

   Configure queue out to PQ or WRR, set the proportion of the 8 egress queues bandwidth and mapping from internal priority to egress queue.

6. Configure QoS mapping

   Configure the mapping from CoS to DSCP, DSCP to CoS, DSCP to DSCP mutation, IP precedence to DSCP, and policed DSCP.

1. Enable QoS

Command	Explanation
Global Mode	
mls qos **no mls qos**	Enable/disable QoS function.

2. Configure class map.

Command	Explanation
Global Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.
match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>} **no match {access-group | ip dscp | ip precedence | vlan }**	Set matching criterion (classify data stream by ACL, DSCP, VLAN or priority, etc) for the class map; the "**no match {access-group | ip dscp | ip precedence | vlan }**" command deletes specified matching criterion.

3. Configure a policy map.

Command	Explanation

Global Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create a policy map and enter policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
class <*class-map-name*> **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the "**no class <*class-map-name*>**" command deletes the specified class.
set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>} **no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**	Assign a new DSCP and IP precedence value for the classified traffic; the "**no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**" command cancels the newly assigned value.
police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}] **no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**	Configure a policy to classify traffic, data stream exceeding the limit will be dropped or degraded; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.
mls qos aggregate-policer <*aggregate-policer-name*> <*rate-kbps*> <*burst-kbyte*> exceed-action {drop |policed-dscp-transmit} **no mls qos aggregate-policer <*aggregate-policer-name*>**	Define a policy set, perform different actions to out-of-profile data streams, such as discard or degrade. This policy can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.
police aggregate <*aggregate-policer-name*> **no police aggregate <*aggregate-policer-name*>**	Apply a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy set.

4. Apply QoS to ports

Command	Explanation
Interface Mode	
mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]|ip-precedence [pass-through cos]|port priority <*cos*>]	Configure port trust; the "**no mls qos trust**" command disables the current trust

no mls qos trust	status of the port.
mls qos cos {<*default-cos*> } **no mls qos cos**	Configure the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	Apply a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port. Egress policy map is not supported yet.
mls qos dscp-mutation <*dscp-mutation-name*> **no mls qos dscp-mutation <*dscp-mutation-name*>**	Apply DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

5. Configure queue out method and weight

Command	Explanation
Interface Mode	
queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> **noqueue bandwidth**	Set the WRR weight for specified egress queue; the "**no wrr-queue bandwidth**" command restores the default setting.
queue mode strict **priority-queue out** **no priority-queue out**	Configure queue out method to pq method; the "**no priority-queue out**" command restores the default WRR queue out method.
queue mode wrr	restores the default WRR queue out method
Global Mode	
wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*> **no wrr-queue cos-map**	Set CoS value mapping to specified egress queue; the "**no wrr-queue cos-map**" command restores the default setting.

6. Configure QoS mapping

Command	Explanation
Global Mode	

mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>} **no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**	Set CoS to DSCP mapping, DSCP to CoS mapping, DSCP to DSCP mutation mapping, IP precedence to DSCP and policed DSCP mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

13.1.2.2 QoS Configuration Commands

13.1.2.2.1 mls qos

Command: mls qos

no mls qos

Function: Enables QoS in Global Mode; the "**no mls qos**" command disables the global QoS.

Command mode: Global Mode

Default: QoS is disabled by default.

Usage Guide: QoS provides 8 queues to handle traffics of 8 priorities. This function cannot be used with the traffic control function.

Example: Enable/disable QoS function.

Switch(Config)#mls qos

Switch(Config)#no mls qos

13.1.2.2.2 class-map

Command: class-map <*class-map-name*>

no class-map <*class-map-name*>

Function: Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.

Parameter: <*class-map-name*> is the class map name.

Default: No class map is configured by default.

Command mode: Global Mode

Example: Create and delete a class map named "c1".

Switch(Config)#class-map c1

Switch(Config-ClassMap)# exit
Switch(Config)#no class-map c1

13.1.2.2.3 match

Command: match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>}
no match {access-group | ip dscp | ip precedence | vlan }

Function: Configure the matching criterion in the class map: the "**no match {access-group | ip dscp | ip precedence | vlan }**" command deletes the specified matching criterion.

Parameter: access-group <*acl-index-or-name*> stands for matching specified ACL, the parameter is ACL number or name; **ip dscp <*dscp-list*>** stands for matching specified DSCP value, the parameter is a DSCP value list containing up to 8 DSCP values; **ip precedence <*ip-precedence-list*>** stands for matching specified IP priority, the parameter is a IP priority list containing up to 8 IP priorities, ranging from 0 to 7; **vlan <*vlan-list*>** stands for matching specified VLAN ID list consisting of up to 8 VLAN Ids.;

Default: No matching criterion is configured by default.

Command mode: Class map configuration mode

Usage Guide: Only one matching criterion is allowed in each class map. When matching ACL, only "permit" rule can be set in the ACL.

Example: Create a class map named c1, set the class map rule to match packets of IP precedence priority 0 and 1.

Switch(Config)#class-map c1
Switch(Config-ClassMap)#match ip precedence 0 1
Switch(Config-ClassMap)#exit

13.1.2.2.4 policy-map

Command: policy-map <*policy-map-name*>
no policy-map <*policy-map-name*>

Function: Create a policy map and enter the policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.

Parameter: < *policy-map-name*> is the policy map name.

Default: No policy map is configured by default.

Command mode: Global Mode

Usage Guide: QoS classification matching and marking operations can be done in the

policy map configuration mode.

Example: Create and delete a policy map named “p1”.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#exit

Switch(Config)#no policy-map p1

13.1.2.2.5 class

Command: class <class-map-name>

no class <*class-map-name*>

Function: Associate a class to a policy map and enter the policy class map mode; the “**no class <*class-map-name*>**” command deletes the specified class.

Parameter: < *class-map-name*> is the class map name used by the class.

Default: No policy class is configured by default.

Command mode: Policy map configuration Mode

Usage Guide: Before setting up a policy class, a policy map should be created and the policy map mode entered; in the policy map mode, classification and policy configuration can be performed on packet traffic classified by class map.

Example: Enter a policy class mode.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config--Policy-Class)#exit

13.1.2.2.6 set

Command: set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}

no set {ip dscp | ip precedence}

Function: Assign a new DSCP and IP precedence value for the classified traffic; the “**no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**” command cancels the newly assigned value.

Parameter: <*new-dscp*> is the new DSCP value; **<*new-precedence*>** is the new IP precedence value.

Default: No value is assigned by default.

Command mode: Policy class map configuration Mode

Usage Guide: Only traffic satisfies the matching criterion and those classified will be assigned new values.

Example: Set the IP Precedence value of packets satisfying c1 class rule to 3.

Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#set ip precedence 3
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit

13.1.2.2.7 police

Command: police *<rate-kbps>* *<burst-kbyte>* [exceed-action {drop | policed-dscp-transmit}]

no police *<rate-kbps>* *<burst-kbyte>* [exceed-action {drop | policed-dscp-transmit}]

Function: Configure a policy to a classified traffic; the "**no police *<rate-kbps>* *<burst-kbyte>* [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.

Parameter: *<rate-kbps>* is the average baud rate (in kb/s) of classified traffic, range from 1,000 to 10,000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: There is no policy by default.

Command mode: Policy class map configuration Mode

Usage Guide: The ranges of ***<rate-kbps>*** and ***<burst-kbyte>*** are quite large, if the setting exceeds the actual speed of the port, the policy map applying this policy will not bind to switch ports.

Example: Set the bandwidth for packets that matching c1 class rule to 20 MB/s, with a burst value of 2 MB, all packets exceed this bandwidth setting will be dropped.

Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#police 20000 2000 exceed-action drop
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit

13.1.2.2.8 mls qos aggregate-policer

Command: mls qos aggregate-policer *<aggregate-policer-name>* *<rate-kbps>* *<burst-kbyte>* exceed-action {drop |policed-dscp-transmit}

no mls qos aggregate-policer <*aggregate-policer-name*>

Function: Define a policy set that can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.

Parameter: <*aggregate-policer-name*> is the name of the policy set; **<*rate-kbps*>** is the average baud rate (in kb/s) of classified traffic, range from 1,000 to 10,000,000; **<*burst-kbyte*>** is the burst value (in kb/s) for classified traffic, range from 1 to 1,000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: No policy set is configured by default.

Command mode: Global Mode

Usage Guide: If a policy set is using by a policy map, it cannot be deleted unless the reference to the policy set is cleared in the appropriate policy map with "**no police aggregate <*aggregate-policer-name*>**" command. The delete should be performed in Global Mode with "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command.

Example: Set a policy set named "agg1", the policy set defines the bandwidth for packets to 20 MB/s, with a burst value of 2 MB, all packets exceeding this bandwidth setting will be dropped.

Switch(Config)#mls qos aggregate-policer agg1 20000 2000 exceed-action drop

13.1.2.2.9 police aggregate

Command: police aggregate <*aggregate-policer-name*>

no police aggregate <*aggregate-policer-name*>

Function: Apply a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy set.

Parameter: <*aggregate-policer-name*> is the policy set name.

Default: No policy set is configured by default.

Command mode: Policy class map configuration Mode

Usage Guide: The same policy set can be referred to by different policy class maps.

Example: Apply policy set "agg1" to packets satisfying c1 class rule.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config--Policy-Class)#police aggregate agg1

Switch(Config--Policy-Class)#exit

Switch(Config-PolicyMap)#exit

13.1.2.2.10 mls qos trust

Command: mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]| ip-precedence [pass-through-cos] |port priority <*cos*>]
[no] mls qos trust

Function: Configure port trust; the "**no mls qos trust**" command disables the current trust status of the port.

Parameter: cos configures the port to trust CoS value; **cos pass-through-dscp** configures the port to trust CoS value but does not change packet DSCP value; **dscp** configures the port to trust DSCP value; **dscp pass-through-cos** configures the port to trust DSCP value, but does not change packet CoS value; **ip-precedence** configures the port to trust IP precedence; **ip-precedence pass-through-cos** configures the port to trust IP precedence, but does not change packet CoS value.

port priority <*cos*> assign a priority to the physical port, **cos** is the priority to assign. Priority of all incoming packets through the port will be set to this cos value. This is irrelevant to the priority of the packet itself, no modification is done to the packets.

Default: No trust.

Command mode: Interface Mode

Usage Guide: For packets with both CoS value and DSCP value, keyword **pass-through** should be used to protect the value if the value should not be changed after classification.

Example: Configure port ethernet 1/1 to trust CoS value, i.e. classify the packets according to CoS value, DSCP value should not be changed.

Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#mls qos trust cos pass-through-dscp

13.1.2.2.11 mls qos cos

Command: mls qos cos {<*default-cos*> }
no mls qos cos

Function: Configure the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.

Parameter: < *default-cos*> is the default CoS value for the port, the valid range is 0 to 7.

Default: The default CoS value is 0.

Command mode: Interface Mode

Example: Set the default CoS value of port ethernet 1/1 to 5, i.e., packets coming in through this port will be assigned a default CoS value of 5 if no CoS value present.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos cos 5

13.1.2.2.12 service-policy

Command: service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function: Apply a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port.

Parameter: input <*policy-map-name*> applies the specified policy map to the ingress of switch port; **output <*policy-map-name*>** applies the specified policy map to the egress of switch port.

Default: No policy map is bound to ports by default.

Command mode: Interface Mode

Usage Guide: Configuring port trust status and applying policy map on the port are two conflicting operations, the later configuration will override the earlier configuration, only one policy map can be applied to each direction of each port. Egress policy map is not supported yet.

Example: Bind policy p1 to ingress of port ethernet 1/1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)# service-policy input p1

13.1.2.2.13 mls qos dscp-mutation

Command: mls qos dscp-mutation <*dscp-mutation-name*>

no mls qos dscp-mutation <*dscp-mutation-name*>

Function: Apply DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

Parameter: <*dscp-mutation-name*> is the DSCP mutation mapping name.

Default: There is no policy by default.

Command mode: Interface Mode

Usage Guide: For configuration of DSCP mutation mapping on the port to take effect, the trust status of that port must be “trust DSCP”. Applying DSCP mutation mapping allows DSCP value specified directly convert to new DSCP value without class and policy process. DSCP mutation mapping is effective to the local port only, “trust DSCP” refers to the DSCP value before DSCP mutation in this case.

Example: Configure port ethernet 1/1 to trust DSCP, using DSCP mutation mapping of mu1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust dscp pass-through cos

Switch(Config-Ethernet1/1)#mls qos dscp-mutation mu1

13.1.2.2.14 queue bandwidth

Command: queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*>

no queue bandwidth

Function: Set the WRR weight for specified egress queue; the “**no wrr-queue bandwidth**” command restores the default setting.

Parameter: <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> are WRR weights, ranging from 0 to 15.

Default: The default values of weight1 to weight8 are 1 through 8. .

Command mode: Interface Mode

Usage Guide: The absolute value of WRR is meaningless. WRR allocates bandwidth by the proportion the eight weight values. If a weight is 0, then the queue has the highest priority; when the weights of multiple queues are set to 0, then the queue of higher order has the higher priority.

Example: Set the bandwidth weight proportion of the eight queue out to be 1: 1: 2: 2: 4: 4: 8: 8.

Switch(Config-Ethernet1/1)# queue bandwidth 1 1 2 2 4 4 8 8

13.1.2.2.15 queue mode

Command: queue mode strict

queue mode wrr

Function: Queue mode strict configure the queue out. Configure the queue to the output queue **queue mode wrr** restores wrr queue out

Default: non-queue mode.

Command mode: Interface Mode

Usage Guide: When queue queue out mode is used, packets are no longer sent with WRR weighted algorithm, but send packets queue after queue.

Example: Set the queue out mode to queue.

Switch(Config-Ethernet1/1)# queue mode strict

13.1.2.2.16 wrr-queue cos-map

Command: wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>

no wrr-queue cos-map

Function: Set the CoS value mapping to the specified queue out; the "**no wrr-queue cos-map**" command restores the default setting.

Parameter: <*queue-id*> is the ID of queue out, ranging from 1 to 8; **<*cos1 ... cos8*>** are CoS values mapping to the queue out, ranging from 0 – 7, up to 8 values are supported.

Default:

Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	0	1	2	3	4	5	6	7
Queue Selected	1	2	3	4	5	6	7	8

Command mode: Global Mode

Usage Guide:

Example: Map packets with CoS value 2 and 3 to egress queue 1.

Switch(Config)#wrr-queue cos-map 1 2 3

13.1.2.2.17 mls qos map

Command: mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>}

no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}

Function: Set **class of service (CoS)-to-Differentiated Services Code Point (DSCP)**

mapping, **DSCP to CoS** mapping, **DSCP to DSCP mutation** mapping, **IP precedence to DSCP** and **policed DSCP** mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

Parameter: **cos-dscp <*dscp1...dscp8*>** defines the mapping from CoS value to DSCP, **<*dscp1...dscp8*>** are the 8 DSCP value corresponding to the 0 to 7 CoS value, each DSCP value is delimited with space, ranging from 0 to 63; **dscp-cos <*dscp-list*> to <*cos*>** defines the mapping from DSCP to CoS value, **<*dscp-list*>** is a list of DSCP value consisting of up to 8 DSCP values, **<*cos*>** are the CoS values corresponding to the DSCP values in the list; **dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** defines the mapping from DSCP to DSCP mutation, **<*dscp-mutation-name*>** is the name for mutation mapping, **<*in-dscp*>** stand for incoming DSCP values, up to 8 values are supported, each DSCP value is delimited with space, ranging from 0 to 63, **<*out-dscp*>** is the sole outgoing DSCP value, the 8 values defined in incoming DSCP will be converted to outgoing DSCP values; **ip-prec-dscp <*dscp1...dscp8*>** defines the conversion from IP precedence to DSCP value, **<*dscp1...dscp8*>** are 8 DSCP values corresponding to IP precedence 0 to 7, each DSCP value is delimited with space, ranging from 0 to 63; **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** defines DSCP **mark down** mapping, where **<*dscp-list*>** is a list of DSCP values containing up to 8 DSCP values, **<*mark-down-dscp*>** are DSCP value after **mark down**.

Default: Default mapping values are:

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation and policed-dscp are not configured by default

Command mode: Global Mode

Usage Guide: In **police** command, classified packet traffic can be set to mark down if exceed specified average speed or burst value, **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** can mark down the DSCP values of those packets to new DSCP values.

Example: Set the ***CoS-to-DSCP*** mapping value to the default 0 8 16 24 32 40 48 56 to 0

1 2 3 4 5 6 7.

Switch(Config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

13.1.3 QoS Example

Scenario 1:

Enable QoS function, change the queue out weight of port ethernet 1/1 to 1: 1: 2: 2: 4: 4: 8: 8, and set the port in trust CoS mode without changing DSCP value, and set the default CoS value of the port to 5.

The configuration steps are listed below:

Switch#config
Switch(Config)#mls qos
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# queue bandwidth 1 1 2 2 4 4 8 8
Switch(Config-Ethernet1/1)#mls qos trust cos pass-through dscp
Switch(Config-Ethernet1/1)#mls qos cos 5

Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet 1/1 is 1: 1: 2: 2: 4: 4: 8: 8. When packets have CoS value coming in through port ethernet 1/1, it will be map

to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8, respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue 6. All passing packets would not have their DSCP values changed.

Scenario 2:

In port ethernet 1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.

The configuration steps are listed below:

Switch#config

Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(Config)#mls qos

Switch(Config)#class-map c1

Switch(Config-ClassMap)#match access-group 1

Switch(Config-ClassMap)# exit

Switch(Config)#policy-map p1

```
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#police 10000 4000 exceed-action drop
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit
Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet1/2)#service-policy input p1
```

Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet 1/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Scenario 3:

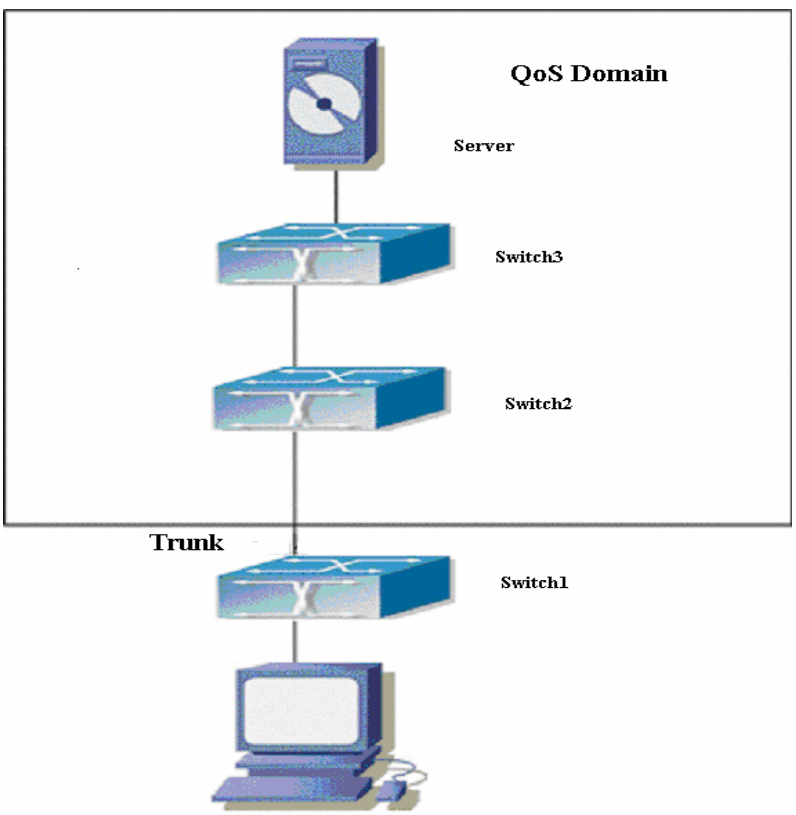


Fig 13-3 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, switch1` classifies different traffic and assigns different IP precedence. For example, set IP precedence for packets from segment 192.168.1.0 to 5 on port ethernet 1/1. The port connecting to switch2 is a trunk port. In Switch2, set port ethernet 1/1 that connecting to swtich1 to trust IP

precedence. Thus inside the QoS domain, packets of different priority will go to different queues and get different bandwidth.

The configuration steps are listed below:

QoS configuration in Switch1:

```
Switch#config
Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(Config)#mls qos
Switch(Config)#class-map c1
Switch(Config-ClassMap)#match access-group 1
Switch(Config-ClassMap)# exit
Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#set ip precedence 5
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#service-policy input p1
```

QoS configuration in Switch2:

```
Switch#config
Switch(Config)#mls qos
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#mls qos trust ip-precedence pass-through-cos
```

13.1.4 QoS Troubleshooting Help

13.1.4.1 QoS Debug and Monitor Commands

13.1.4.1.1 show mls-qos

Command: show mls-qos

Function: Display global configuration information for QoS.

Parameter: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide: This command indicates whether QoS is enabled or not.

Example:

Switch #show mls-qos

Qos is enabled

Displayed information	Explanation
Qos is enabled	QoS is enabled.

13.1.4.1.2 show mls qos aggregate-policer

Command: show mls qos aggregate-policer [<*aggregate-policer-name*>]

Function: Display policy set configuration information for QoS.

Parameter: <*aggregate-policer-name*> is the policy set name.

Default: N/A.

Command mode: Admin Mode

Example:

Switch #show mls qos aggregate-policer policer1

aggregate-policer policer1 80000 80 exceed-action drop

Not used by any policy map

Displayed information	Explanation
aggregate-policer policer1 80000 80 exceed-action drop	Configuration for this policy set.
Not used by any policy map	Time of this policy set being referred to .

13.1.4.1.3 show mls qos interface

Command: show mls qos interface [<*interface-id*>] [buffers | policers | queueing | statistics]

Function: Display QoS configuration information on a port.

Parameter: <***interface-id***> is the port ID; **buffers** is the queue buffer setting on the port; **policers** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Statistics are available only when ingress policy is configured.

Example:

Switch #show mls qos interface ethernet 1/2

Ethernet1/2

default cos: 0

DSCP Mutation Map: Default DSCP Mutation Map

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
default cos: 0	Default CoS value of the port.
DSCP Mutation Map: Default DSCP Mutation Map	Port DSCP map name
Attached policy-map for Ingress: p1	Name of the policy bound to the port.

Switch # show mls qos interface buffers ethernet 1/2

Ethernet1/2

packet number of 8 queue:

0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200

Displayed information	Explanation
packet number of 8 queue: 0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200	Available packet number for all 8 queues out on the port, this is a fixed setting that cannot be changed.

Switch # show mls qos interface queueing ethernet 1/2

Switch#show mls qos int queue e 1/2

Cos-queue map:

Cos 0 1 2 3 4 5 6 7

Queue 1 2 3 4 5 6 7 8

Queue and weight type:

Port q1 q2 q3 q4 q5 q6 q7 q8 QType

Ethernet1/2 1 2 3 4 5 6 7 8 WFQ

Displayed information	Explanation
Cos-queue map:	CoS value to queue mapping.

Queue and weight type:	Queue to weight mapping.
QType	WFQ or PQ queue out method

Switch # show mls qos interface policers ethernet 1/2

Ethernet1/2

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
Attached policy-map for Ingress: p1	Policy map bound to the port.

Switch # show mls qos interface statistics ethernet 1/2

Device: Ethernet1/2

Classmap classified in-profile out-profile (in packets)

c1 0 0 0

Displayed information	Explanation
Ethernet1/2	Port name
ClassMap	Name of the Class map
classified	Total data packets match this class map.
in-profile	Total in-profile data packets match this class map.
out-profile	Total out-profile data packets match this class map.

13.1.4.1.4 show mls qos maps

Command: show mls qos maps [cos-dscp | dscp-cos | dscp-mutation *<dscp-mutation-name>* | ip-prec-dscp | policed-dscp]

Function: Display mapping configuration information for QoS.

Parameter: cos-dscp CoS for CoS-DSCP; **dscp-cos** DSCP for DSCP-CoS, **dscp-mutation *<dscp-mutation-name>*** for DSCP-DSCP mutation, ***<dscp-mutation-name>*** is the name of mutation; **ip-prec-dscp** IP for IP precedence-DSCP; **policed-dscp** is DSCP mark down mapping.

Default: N/A.

Command mode: Admin Mode

Example:

Switch # show mls qos map

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

IpPrecedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

Dscp-cos map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

Policed-dscp map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	1	2	3	4	5	6	7	8	9
1:	10	11	12	13	14	15	16	17	18	19
2:	20	21	22	23	24	25	26	27	28	29
3:	30	31	32	33	34	35	36	37	38	39
4:	40	41	42	43	44	45	46	47	48	49
5:	50	51	52	53	54	55	56	57	58	59
6:	60	61	62	63						

13.1.4.1.5 show class-map

Command: show class-map [<*class-map-name*>]

Function: Display class map of QoS.

Parameter: < *class-map-name*> is the class map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Display all configured class-map or specified class-map information.

Example:

Switch # show class-map

Class map name: c1

Match acl name: 1

Displayed information	Explanation
Class map name: c1	Name of the Class map
Match acl name: 1	Classifying rule for the class map.

13.1.4.1.6 show policy-map

Command: show policy-map [<*policy-map-name*>]

Function: Display policy map of QoS.

Parameter: < *policy-map-name*> is the policy map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Display all configured policy-map or specified policy-map information.

Example:

Switch # show policy -map

Policy Map p1

Class Map name: c1

police 16000000 2000 exceed-action drop

Displayed information	Explanation
Policy Map p1	name of policy map
Class map name: c1	Name of the class map referred to
police 16000000 8000 exceed-action drop	Policy implemented

13.1.4.2 QoS Troubleshooting Help

- ☞ QoS is disabled on switch ports by default, 8 sending queues are set by default, queue1 forwards normal packets, other queues are used for some important control packets (such as BPDU).
- ☞ When QoS is enabled in Global Mode, QoS is enabled on all ports with 8 traffic queues. The default CoS value of the port is 0; port is in not Trusted state by default; the default queue weight values are 1, 2, 3, 4, 5, 6, 7, 8 in order, all QoS Map is using the default value.
- ☞ CoS value 7 maps to queue 8 that has the highest priority and usually reserved for certain protocol packets. It is not recommended for the user to change the mapping between CoS 7 to Queue 8, or set the default port CoS value to 7.

- ☞ Policy map can only be bound to ingress direction, egress is not supported yet.
- ☞ If the policy is too complex to be configured due to hardware resource limit, error massages will be provided.

13.1.5 Web Management

Select **QoS configuration** and it consist of six sections as following:

- Enable QoS
- Class-map configuration
- Policy-map configuration
- Apply QoS to port
- Egress-queue configuration
- QoS mapping configuration

13.1.5.1 Enable QoS

Click Enable QoS to display the extension, select Enable/Disable QoS then entry the configure page. It is equivalent to CLI command 13.1.2.2.1.

All sections describe as following:

- QoS status－Close or Enable.

To enable QoS, select Enable, then click Apply.



13.1.5.2 Class-map Configuration

Click Class-map configuration to display the extension, including two sections:

1. Add/Remove class-map
2. Class-map configuration

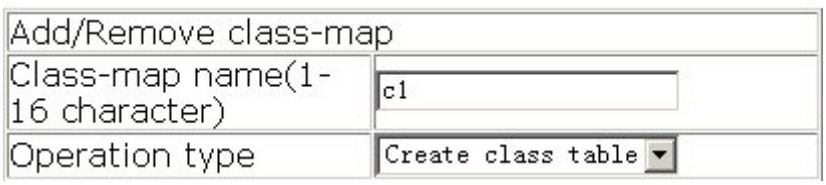
13.1.5.2.1 Add/Remove Class-map

Click Add/Remove class-map then entry the configure page. It is equivalent to CLI command 13.1.2.2.2.

All sections describe as following:

- Class - map name
- Operation type－Create class table and Remove class table.

Adding class-map name, specify the class-map name, select Create class table, then click Apply.



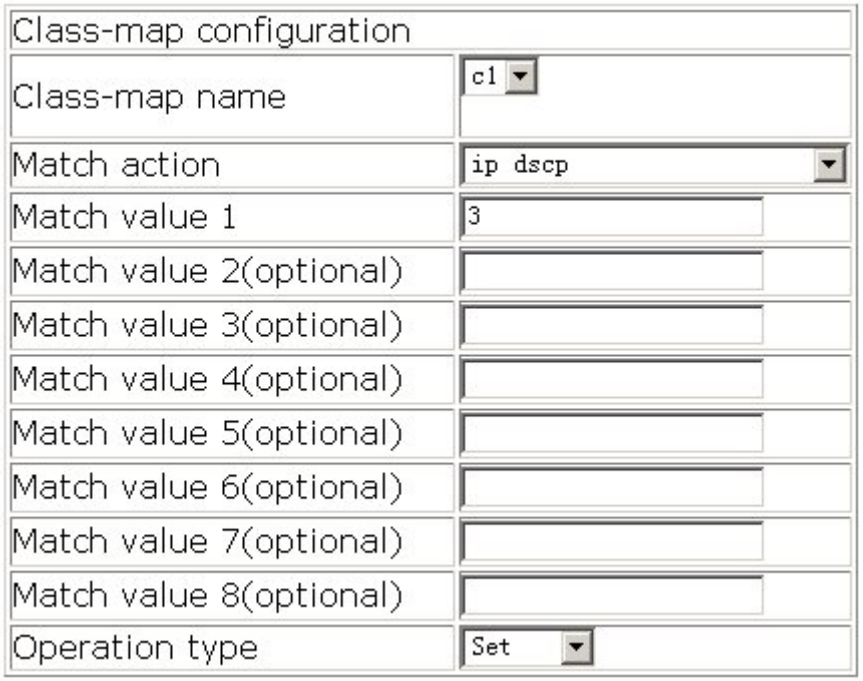
13.1.5.2.2 Class-map Configuration

Click Class-map configuration then entry the configure page. It is equivalent to CLI command 13.1.2.2.3.

All sections describe as following:

- Class-map name
- Match action which including:
  - ✓ **access-group First valid**－mapping to ACL table. Parameter is the assign number or name of ACL. First valid means Match value 1 is valid.
  - ✓ **ip dscp**－mapping to DSCP. Parameter is the DSCP value list.
  - ✓ **ip precedence**－mapping to IP priority. Parameter is IP priority value list.
  - ✓ **vlan**－mapping to VLAN ID. Parameter is VLAN ID value list.
  - ✓ **Match value 1-8**－mapping to parameter value table. Input ACL value to Match value 1 for mapping ACL.
  - ✓ **Operation type**－Set or Remove.

To configure Class-map c1, select c1 to Class-map name, select ip dscp to Match action, input 3 to Match value 1, select set to Operation type, then click Apply.



13.1.5.3 Policy-map Configuration

Click Policy-map configuration to display the extension, including five sections:

- Add/Remove policy-map
- Policy-map priority configuration
- Policy-map bandwidth configuration
- Add/Remove aggregate policer
- Apply aggregate policer

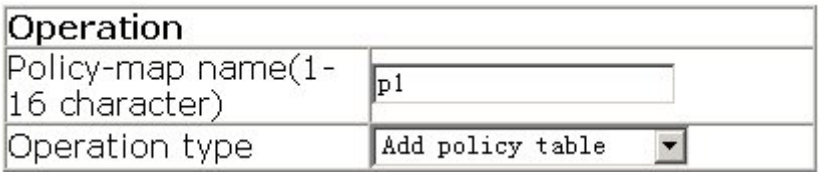
13.1.5.3.1 Add/Remove Policy-map

Click Add/Remove policy-map then entry the configure page. It is equivalent to CLI command 13.1.2.2.4.

All sections describe as following:

- Policy-map name
- Operation type. Add policy table or Remove policy table.

Setting policy-map name as p1, select Add policy table, then click Apply to add policy table.



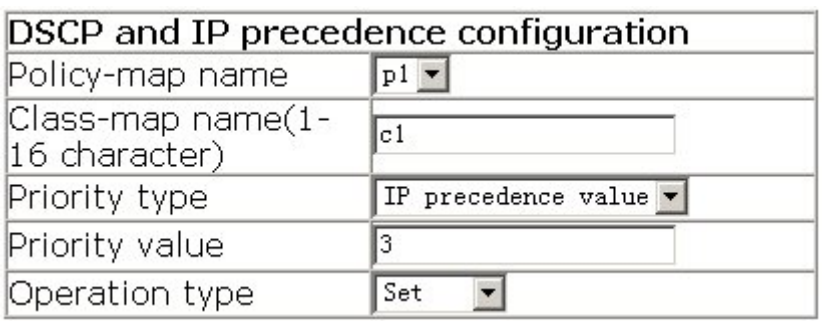
13.1.5.3.2 Policy-map Priority Configuration

Click Policy-map priority configuration to entry configure page. It is equivalent to CLI command 13.1.2.2.6.

All sections describe as following:

- Policy-map name
- Class-map name
- Priority type. DSCP value or IP precedence value
- Priority value
- Operation type. Set or Remove.

To configure Policy-map priority, select p1 to Policy-map name, input c1 to Class-map name, select IP precedence value to Priority type, input 3 to Priority value, select Set to Operation type, then click Apply.



13.1.5.3.3 Policy-map Bandwidth Configuration

Click Policy-map bandwidth configuration to entry configure page. It is equivalent to CLI command 13.1.2.2.7.

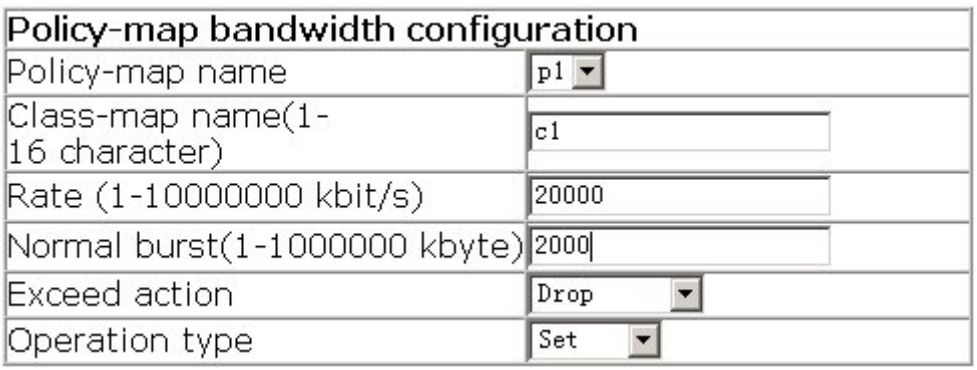
All sections describe as following:

- Policy-map name
- Class-map name
- Rate—average baud rate for classified bandwidth, K bit/s per unit.
- Normal burst—burst rate for classified bandwidth, K byte per unit.
- Exceed action—The action for once the data rate exceeds the rate limited, includes

drop and policied-dscp-transmit, the latter is by a mapping function between given DSCP and corresponding policy and mark the DSCP into the packet.

- Operation type－Set or Remove.

To configure Policy-map bandwidth configuration, select p1 to Policy-map name, input c1 to Class-map name, all sections choose as default setting, select Set to Operation type, then click Apply.



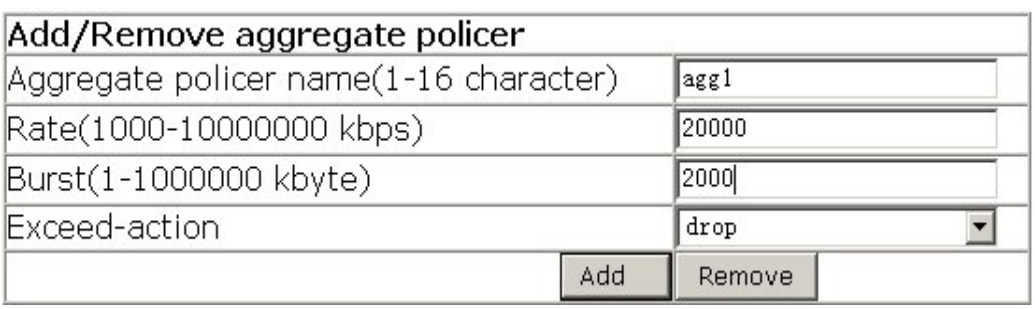
13.1.5.3.4 Add/Remove Aggregate Policer

Click Add/Remove aggregate policer to entry configure page. I is equivalent to CLI command 13.1.2.2.8.

All sections describe as following:

- Aggregate policer name
- Rate－average baud rate for classified bandwidth, K bit/s per unit.
- Burst－burst rate for classified bandwidth, K byte per unit.
- Exceed-action－The action for once the data rate exceeds the rate limited, includes drop and policied-dscp-transmit, the latter is by a mapping function between given DSCP and corresponding policy and mark the DSCP into the packet.

To create the aggregate-policer, named as agg1, the definition of aggregate-policer is based on the baud rate 20M Kbps, the burst rate 2M Kbyte. All packets will be dropped whenever over the assigned running rate. After setting all value, then click Add.



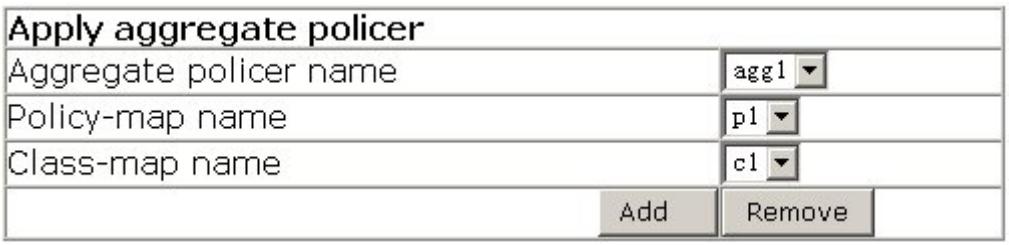
13.1.5.3.5 Apply Aggregate Policer

Click Apply aggregate policer to entry the configure page. It is equivalent to CLI command 13.1.2.2.9.

All sections describe as following:

- Aggregate policer name
- Policy-map name
- Class-map name

To apply the aggregate policer agg1 by c1 class-map, input the graphic presentation value, then click Add.



13.1.5.4 Apply QoS to Port

Click Apply QoS to port to entry the configure page, including four sections:

- Port trust mode configuration
- Port default CoS configuration
- Apply policy-map to port
- Apply DSCP mutation mapping

13.1.5.4.1 Port Trust Mode Configuration

Click Port trust mode configuration to entry the configure page. It is equivalent to CLI command 13.1.2.2.10.

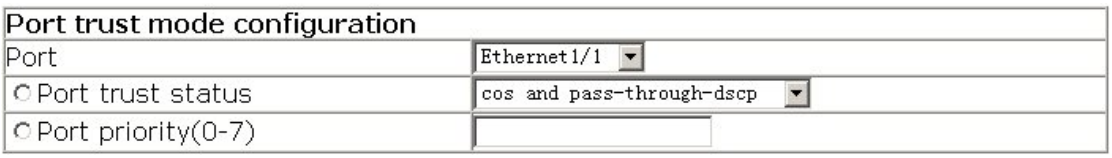
All sections describe as following:

- Port
- Port trust status－including
  - ✓ cos, cos and pass-through-dcsp,
  - ✓ dcsp, dcsp and pass-through-cos,
  - ✓ ip-precedence, ip-pre and pass-through-cos
- Port priority
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.

- Default－Will back to startup setting. This command will modify the configuration.

The parameter will take effect alternative port trust status and port priority.

To configure the port Ethernet 1/1 with trust mode, should set the packet by COS value classification first and keep it without changing DSCP value. Choosing the Ethernet1/1 port and select the cos and pass-through-dcsp for Port trust status, then click Apply.



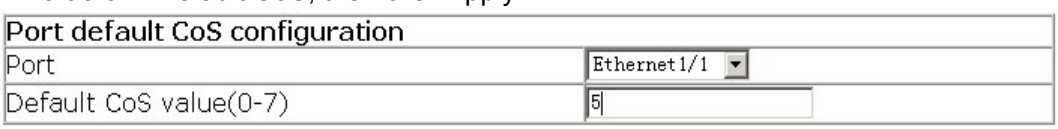
13.1.5.4.2 Port Default Cos Configuration

Click Port default CoS configuration to entry configure page. It is equivalent to CLI command 13.1.2.2.11.

All sections describe as following:

- Port
- Default CoS value－Startup CoS value
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.
- Default－Will back to startup setting. This command will modify the configuration.

If would like to set the cos value 5 in port Ethernet 1/1. Selecting port Ethernet1/1, input value 5 in Default CoS, then click Apply.



13.1.5.4.3 Apply Policy-map to Port

Click Apply policy-map to port to entry the configure page. It is equivalent to CLI command 13.1.2.2.12.

All sections describe as following:

- Port
- Policy-map name
- Port direction－Input or Output

- Operation－Set or Remove
- Reset－Will set column as startup defaults. This command will not modify the configuration.

Apply－Will take effort to all setting. This command will modify the configuration.

If would like to set the policy-map in port Ethernet 1/1. Choosing Ethernet1/1 for port and p1 for policy-map; to select Input for port direction and Set for operation, then click Apply.

Apply policy-map to port	
Port	Ethernet1/1
Policy-map name	p1
Port direction	Input
Operation	Set

13.1.5.4.4 Apply DSCP Mutation Mapping

Click Apply DSCP mutation mapping to entry the configure page. It is equivalent to CLI command 13.1.2.2.13.

All sections describe as following:

- Port name
- DSCP mutation name
- Operation－Set or Remove

If would like to set the DSCP mutation in port Ethernet 1/1. Choosing Port name as Ethernet1/1, input mu1 for DCSP mutation name, to select Set for Operation, then click Apply.

DSCP mutation (the applied port should have DSCP configured)	
Port name	Ethernet1/1
DSCP mutation name(1-16 character)	mu1
Operation	Set

13.1.5.5 Egress-Queue Configuration

Click Egress-queue configuration to display the extensions, including three sections:

1. Egress-queue wrr weight configuration
2. Egress-queue work mode configuration
3. Mapping CoS values to egress queues

13.1.5.5.1 Egress-queue WRR Weight Configuration

Click Egress-queue WRR weight configuration to entry the configure page. It is equivalent to CLI command 13.1.2.2.14.

All sections describe as following:

- Port nameWeight for queue 0-7
- Operation－Set or Remove
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.

To configure the WRR weight should choosing the port name first, then input value for each queue; select Set for operation, then click Apply.

Egress-queue wrr weight configuration	
Port name	Ethernet1/1
Weight for queue0(0-15)	1
Weight for queue1(0-15)	1
Weight for queue2(0-15)	2
Weight for queue3(0-15)	2
Weight for queue4(0-15)	4
Weight for queue5(0-15)	4
Weight for queue6(0-15)	8
Weight for queue7(0-15)	8
Operation	Set

13.1.5.5.2 Egress-queue Work Mode Configuration

Click Egress-queue work mode configuration to entry the configure page. It is equivalent to CLI command 13.1.2.2.15.

All sections describe as following:

- Port name
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.
- Default－Will back to startup setting. This command will modify the configuration.

To configure the port as priority-queue mode should choosing port name first, then click Apply.

Set the egress-queue work mode to priority	
Port name	Ethernet1/1

13.1.5.5.3 Mapping CoS Values to Egress Queue

Click Mapping CoS values to egress queue to entry the configure page. It is equivalent to CLI command 13.1.2.2.16.

All sections describe as following:

- Queue-ID
- CoS value－Mapping CoS values to Egress queue. Up to 8 queue to be supported.
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Default－Will back to startup setting. This command will modify the configuration.

If would like to set the packet with CoS value 2/3 to mapping egress queue 1, the Queue-ID should be set as 1 and CoS value be set with value 2/3, then click Apply.

Mapping CoS values to egress queue	
Queue-ID(1-8)	1
CoS value(0-7)	2
CoS value(0-7)	3
CoS value(0-7)	
CoS value(0-7)	
CoS value(0-7)	
CoS value(0-7)	
CoS value(0-7)	
CoS value(0-7)	

13.1.5.6 QoS Mapping Configuration

Click QoS mapping configuration to display extensions, including sections as following:

1. CoS-to-DSCP mapping
2. DSCP-to-CoS mapping
3. DSCP mutation mapping
4. IP-Precedence-to-DSCP mapping
5. DSCP mark down mapping

These configurations are equivalent to CLI command13.1.2.2.17.

13.1.5.6.1 CoS-to-DSCP Mapping

Click CoS-to-DSCP mapping to entry the configure page.

All sections describe as following:

- CoS－CoS value 0-7
- DSCP－Up to 8 DSCP mutations and mapping to CoS value 0～7

- Operation－Set or Remove

If would like applying CoS value 2 to map DSCP value 20, it should input the DSCP value 20 in CoS value 2 column, selecting Set for Operation type, then click Apply.

CoS-to-DSCP mapping								
CoS value	0	1	2	3	4	5	6	7
DSCP value(0-63)	0	8	20	24	32	40	48	56
Operation type	Set							

13.1.5.6.2 DSCP-to-CoS Mapping

Click DSCP-to-CoS mapping to entry configure page.

All sections describe as following:

- DSCP 1-8－DSCP value
- CoS Value－DSCP value mapping to CoS value
- Operation type－Add or Remove

If would like applying DSCP value 20 mapping to CoS value 2, it should input the CoS value 2 and DSCP1 value 20, selecting Set for Operation type, then click Apply.

DSCP-to-CoS mapping	
DSCP value1(0-63)	20
DSCP value2(optional, 0-63)	
DSCP value3(optional, 0-63)	
DSCP value4(optional, 0-63)	
DSCP value5(optional, 0-63)	
DSCP value6(optional, 0-63)	
DSCP value7(optional, 0-63)	
DSCP value8(optional, 0-63)	
CoS value(0-7)	2
Operation type	Set

13.1.5.6.3 DSCP Mutation Mapping

Click DSCP mutation mapping to entry the configure page.

All sections describe as following:

- DSCP mutation name
- Out-DSCP value
- In-DSCP value1-8
- Operation type－Set or Remove

To configure the DSCP mutation mapping should input the required value first, selecting Set for Operation type, then click Apply.

DSCP mutation mapping	
DSCP mutation name(1-16 character)	mul
Out-DSCP value(0-63)	22
In-DSCP value1(0-63)	33
In-DSCP value2(optional, 0-63)	
In-DSCP value3(optional, 0-63)	
In-DSCP value4(optional, 0-63)	
In-DSCP value5(optional, 0-63)	
In-DSCP value6(optional, 0-63)	
In-DSCP value7(optional, 0-63)	
In-DSCP value8(optional, 0-63)	
Operation type	Set

13.1.5.6.4 IP-Precedence-to-DSCP Mapping

Click IP-Precedence-to-DSCP mapping to entry the configure page.

All sections describe as following:

- IP-Precedence－IP precedence value 0～7
- DSCP－IP precedence value mapping to DSCP value
- Operation type－Set or Remove

If would like to set the IP precedence value 2 mapping to DSCP value 20, it should input the DSCP value 20 in IP precedence value 2 column, selecting Set for Operation type, then click Apply.

IP-Precedence-to-DSCP mapping								
IP-Precedence value	0	1	2	3	4	5	6	7
DSCP value(0-63)	0	8	20	24	32	40	48	56
Operation type	Set							

13.1.5.6.5 DSCP Mark Down Mapping

Click DSCP mark down mapping to entry the configure page.

All sections describe as following:

- Mark down dscp value
- Policed DSCP value1-8－DSCP value table
- Operation type－Set or Remove

If would like to set the DSCP value 10/20 mark down to 30, it should mark down dscp

value 30 first and policed DSCP 1/2 for value10/20, selecting Set for Operation type, then click Apply.

Policed-DSCP mark down mapping	
Mark down DSCP value(0-63)	30
Policed DSCP value1(0-63)	10
Policed DSCP value2(optional, 0-63)	20
Policed DSCP value3(optional, 0-63)	
Policed DSCP value4(optional, 0-63)	
Policed DSCP value5(optional, 0-63)	
Policed DSCP value6(optional, 0-63)	
Policed DSCP value7(optional, 0-63)	
Policed DSCP value8(optional, 0-63)	
Operation type	Set

13.2 PBR

This chapter describes how to configure the PBR through the examples.

13.2.1 PBR Introduction

The PBR (Policy-Based Routing) allows modifying the next hop of the packets according to IP source address, IP destination address, IP precedence, ToS, IP protocol, source port number and destination port number etc.

13.2.2 PBR Configuration

13.2.2.1 PBR Configuration Step

1. Enable the PBR

When the QoS is enabled and disabled globally, the PBR is enabled and disabled automatically.

2. Configure the class-map

Create a classification policy in order to use different policies for different traffic.

3. Configure the policy-map

Create the policy-map. Then correspond the policy-map to the class-map. Enter the policy-map mode and set the next hops for different traffic.

4. Apply the policy to the port.

The policy has to apply to the port.

13.2.2.2 PBR Command

13.2.2.2.1 mls qos

Commands: mls qos

no mls qos

Function: Enable the QoS globally, and the PBR is enabled automatically; The command "**no mls qos**" disables the QoS and the PBR globally.

Command mode: Global Mode

Default: The PBR is disabled.

Usage Guide: When the QoS is enabled, the PBR is enabled automatically. But the PBR can't be enabled independently.

Example: Enable and disable the QoS and the PBR.

Switch(config)#mls qos

Switch(config)#no mls qos

13.2.2.2.2 class-map

Command: class-map <*class-map-name*>

no class-map <*class-map-name*>

Function: Create a class-map and enter class-map mode; The command "**no class-map <*class-map-name*>**" deletes the specified class-map.

Parameter: <*class-map-name*> sets class-map name.

Default: By default, there is no class-map.

Command Mode: Global Mode

Example: Create and delete a class-map called c1.

Switch(config)#class-map c1

Switch(config-ClassMap)# exit

Switch(config)#no class-map c1

13.2.2.2.3 match

Command: match {access-group <*acl-index-or-name*>}

no match {access-group}

Function: Set the match for the class-map; The command "**no match {access-group}**"

deletes the specified match.

Parameter: access-group <*acl-index-or-name*> specifies the ACL. The attribute is the ACL number or name.

Default: By default, there is no match.

Command mode: Class-map Mode

Usage Guide: Only one match can be set in one class-map. When the ACL applies to the PBR, the actions of permit and deny are to specify the next hop or not to specify the next hop when IP messages meet the match. The ACLs which apply to the PBR are indifferent to the order because the deny action is superior to the permit action.

Example: Create a class-map called c1. Set the match policy of this class-map to the ACL called c1

Switch(config)#class-map c1

Switch(config-ClassMap)#match access-group acl1

Switch(config-ClassMap)#exit

13.2.2.2.4 policy-map

Command: policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Function: Create a policy-map and enter policy-map mode; The command "**no policy-map <*policy-map-name*>**" deletes the specified policy-map.

Parameter: <*policy-map-name*> sets the policy-map name.

Default: By default, there is no policy-map.

Command mode: Global Mode

Usage Guide: After entering the policy-map mode, users can set actions for the PBR.

Example: Create and delete a policy-map called p1.

Switch(config)#policy-map p1

Switch(config-PolicyMap)#exit

Switch(config)#no policy-map p1

13.2.2.2.5 class

Command: class <class-map-name>

no class <*class-map-name*>

Function: Enter a policy-map class and enter policy-map mode; The command "**no class <*class-map-name*>**" deletes the specified policy-map.

Parameter: < *class-map-name* > sets the policy-map name.

Default: By default, there is no policy-map.

Command mode: Policy-map Mode

Usage Guide: Before create a policy-map class, users must create a policy-map and enter the policy mode; Inside a policy-map, users can set the next hop according to the traffic. The priority of the classes is decided by the sequence of configuration. For example, if class c1 is configured before class c2, c1 has high priority than c2.

Example: Enter a policy-map mode.

Switch(config)#policy-map p1

Switch(config-PolicyMap)#class c1

Switch(config--Policy-Class)#exit

13.2.2.2.6 set

Command: set {ip nexthop <*nexthop-ip*>}

no set {ip nexthop}

Function: Set the next hop IP address for the sorted traffic; The command "**no set {ip nexthop}**" cancels the next hop setting.

Parameter: <*nexthop-ip*> sets the next hop IP address.

Default: By default, there are no next hop settings.

Command mode: Policy-class Mode

Usage guide: Users can only set the next hop IP address by matching the ACL policy.

Example: Set the next hop to IP address 218.31.1.119 for the traffic which matches the policy called c1.

Switch(config)#policy-map p1

Switch(config-PolicyMap)#class c1

Switch(config--Policy-Class)#set ip nexthop 218.31.1.119

Switch(config--Policy-Class)#exit

Switch(config-PolicyMap)#exit

13.2.2.2.7 service-policy

Command: service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function: Apply a policy-map to a port; The command "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" removes the application of a specified policy-map of the port.

Parameter: input <*policy-map-name*> applies the specified policy-map to the current port for the inbound traffic; **output <*policy-map-name*>** applies the specified policy-map to the current port for the outbound traffic.

Default: By default, there is no bound policy-map.

Command mode: Interface Mode

Usage Guide: The port trust and applied port policy-map are mutually exclusive. The new configuration will replace the previous one. Each port can only apply a policy-map for one direction. The current version of software doesn't support outbound policy-map.

Example: Apply the policy called p1 to the port Ethernet 1/1.

Switch(config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)# service-policy input p1

13.2.3 PBR Example

Example 1:

On the Ethernet port 1/1, set the PBR for the traffic which has the source IP address as 192.168.1.0/24. Set the next hop for the above traffic to 218.31.1.119. For the traffic which has the source IP address as 192.168.1.0/24 and has the destination IP address as 192.168.0.0/16, set not to route it by using the PBR.

The Configuration Procedure is as below:

Switch#config

Switch(config)#ip access-list extended a1

Switch(Config-Ext-Nacl-acl1)#permit ip 192.168.1.0 0.0.0.255 any-destination

Switch(Config-Ext-Nacl-acl1)#deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255

Switch(Config-Ext-Nacl-acl1)#exit

Switch(config)#mls qos

Switch(config)#class-map c1

Switch(config-ClassMap)#match access-group a1

Switch(config-ClassMap)# exit

Switch(config)#policy-map p1

Switch(config-PolicyMap)#class c1

Switch(config-Policy-Class)#set ip nexthop 218.31.1.119

Switch(config--Policy-Class)#exit

Switch(config-PolicyMap)#exit

Switch(config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#service-policy input p1

Configuration Result:

Set the ACL a1 which includes 2 policies. The first policy allows the traffic which has the source IP address as 192.168.1.0/24. The second policy denies the traffic which has the source IP address as 192.168.1.0/24 and has the destination IP address as 192.168.0.0/16. Then, enable the QoS globally. Create a class-map called c1. Set the match for the ACL a1 in the class-map c1. Create a policy-map called p1. Quote c1 in the policy-map p1. Set the next hop IP address as 218.31.1.119. Apply the policy-map p1 on the Ethernet port 1/1.

After the above configuration, on the Ethernet port 1/1, all the traffic which has the source IP address as 192.168.1.0/24, except the traffic which has the source IP address as 192.168.1.0/24 and has the destination IP address as 192.168.0.0/16, is forwarded to 218.31.1.119.

Chapter 14 Layer 3 Forward Configuration

ES4626/ES4650 supports Layer3 forwarding. Layer3 forwarding is to forward Layer3 protocol packets (IP packets) across VLANs. Such forwarding addresses using IP address, when a port receives an IP packet, it will index in its own route table and decide the operation according to the index result. If the IP packet is destined to another subnet reachable from this switch, then the packet will be forwarded from the appropriate port. ES4626/ES4650 can forward IP packets by hardware, the forwarding chip of ES4626/ES4650 has a host route table and default route table. Host route table stores host route connect to the switch directly, default route table stores segment routes (after aggregation algorithm process).

If the route (either host route or segment route) for forwarding unicast traffic exists in the forwarding chip, rather than processing by the CPU in router, the forwarding of traffic will be completely handled by hardware. As a result, forwarding speed can be greatly improved, even to line speed.

14.1 Layer 3 Interface

14.1.1 Introduction to Layer3 Interface

Layer3 interface can be created on ES4626/ES4650. Layer3 interface is not physical interface but a virtual interface. Layer3 interface is built on VLANs. Layer3 interface can contain one or more layer2 interface of the same VLAN, or no layer2 interfaces. At least one of Layer2 interfaces contained in Layer3 interface should be in UP state for Layer3 interface in the UP state, otherwise, Layer3 interface will be in the DOWN state. All layer3 interfaces in the switch use the same MAC address, this address is selected from the reserved MAC address on creating Layer3 interface. Layer3 interface is the base for layer3 protocols. The switch can use the IP address set in layer3 interface to communicate with the other devices via IP. The switch can forward IP packets between different Layer3 interfaces.

14.1.2 Layer3 interface configuration

14.1.2.1 Layer3 Interface Configuration Task Sequence

Create Layer3 Interface

Command	Explanation

Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Create a VLAN interface (VLAN interface is a Layer3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the VLAN interface (Layer3 interface) created in the switch.

14.1.2.2 Layer3 Interface Configuration Commands

14.1.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Create a VLAN interface (a Layer3 interface) ; the "**no interface vlan <*vlan-id*>**" command deletes the Layer3 interface specified.

Parameter: <*vlan-id*> is the VLAN ID of the established VLAN.

Default: No Layer3 interface is configured upon switch shipment.

Command mode: Global Mode

Usage Guide: When crating a VLAN interface (Layer3 interface), VLAN should be configured first, for details, see chapters of VLAN. When VLAN interface (Layer3 interface) is created with this command, VLAN interface (Layer3 interface) configuration mode will be entered. After the creation of VLAN interface(Layer3 interface), interface vlan command can still be used to enter Layer3 interface mode.

Example: Create a VLAN interface (layer3 interface).
Switch (Config)#interface vlan 1

14.2 IP Forwarding

14.2.1 Introduction to IP Forwarding

Gateway devices can forward IP packets from one subnet to another; such forwarding uses the route to find a path. IP forwarding of ES4626/ES4650 is done with the participation of hardware and wire speed forwarding can be achieved. In addition, flexible management is provided to adjust and monitor forwarding. ES4626/ES4650 supports aggregation algorithm enabling/disabling optimization to adjust segment route generation in the switch chip and view statistics for IP forwarding and hardware forwarding chip status.

14.2.2 IP Route Aggregation Configuration

14.2.2.1 IP Route Aggregation Configuration Task

Set whether IP route aggregation algorithm with/without optimization should be used.

1. Set whether IP route aggregation algorithm with/without optimization should be used.

Command	Explanation
ip fib optimize **no ip fib optimize**	Enable the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

14.2.2.2 IP Route Aggregation Configuration Command

14.2.2.2.1 ip fib optimize

Command: ip fib optimize

no ip fib optimize

Function: Enable the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

Default: Disable optimized IP route aggregation algorithm.

Command mode: Global Mode

Usage Guide: This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding virtual default route to the chip segment route table reduces CPU load, it may introduce an unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.

Example: Disable optimized IP route aggregation algorithm.

Switch(Config)# no ip fib optimize

14.2.3 IP Forwarding Troubleshooting Help

14.2.3.1 Monitor and Debug Commands

14.2.3.1.1 show ip traffic

Command: show ip traffic

Function: Display statistics for IP packets.

Command mode: Admin Mode

Usage Guide: Display statistics for IP and ICMP packets received/sent.

Example:

Switch#show ip traffic

IP statistics:

Rcvd: 128 total, 128 local destination

0 header errors, 0 address errors

0 unknown protocol, 0 discards

Frags: 0 reassembled, 0 timeouts

0 fragment rcvd, 0 fragment dropped

0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 0 generated, 0 forwarded

0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded

0 redirects, 0 unreachable, 0 echo, 0 echo replies

0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
Sent: 0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
TcpActiveOpens 0, TcpAttemptFails 0
TcpCurrEstab 0, TcpEstabResets 0
TcpInErrs 0, TcpInSegs 0
TcpMaxConn 0, TcpOutRsts 0
TcpOutSegs 0, TcpPassiveOpens 0
TcpRetransSegs 0, TcpRtoAlgorithm 0
TcpRtoMax 0, TcpRtoMin 0
UDP statics:
UdpInDatagrams 0, UdpInErrors 0
UdpNoPorts 0, UdpOutDatagrams 0

Displayed information	Explanation
IP statistics:	IP packet statistics.
Rcvd: 290 total, 44 local destinations 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent: 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics:	ICMP packet statistics.
Rcvd: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0	Statistics of total ICMP packets received and classified information

quench 0 parameter, 0 timestamp, 0 timestamp replies	
Sent: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

14.2.3.1.2 debug ip packet

Command: debug ip packet
no debug ip packet
Function: Enable the IP packet debug function: the **"no debug IP packet"** command disables this debug function.
Default: IP packet debug information is disabled by default.
Command mode: Admin Mode
Usage Guide: Display statistics for IP packets received/sent, including source/destination address and bytes, etc.
Example: Enable IP packet debug.
Switch#debug ip pa
ip packet debug is on

Switch#
Switch#
Switch#
Switch#%Apr 19 15: 56: 33 2005 IP PACKET: rcvd, src 192.168.2.100, dst 192.168.2.1
, size 60, Ethernet0

14.3 ARP

14.3.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used in IP address to Ethernet MAC address

resolution. ES4626/ES4650 supports both dynamic ARP and static configuration. Furthermore, ES4626/ES4650 supports the configuration of proxy ARP for some applications. For instance, when an ARP request is received on the port, requesting an IP address in the same IP segment of the port but not the same physical network, if the port enabled proxy ARP, the port would reply to the ARP its own MAC address and forward the actual packets received. Enabling proxy ARP allows machines physically separated but of the same IP segment ignores the physical separation and communicate via proxy ARP interface as if in the same physical network.

14.3.2 ARP configuration

14.3.2.1 ARP Configuration Task Sequence

1. Configure static ARP
2. Configure proxy ARP

1. Configure static ARP

Command	Explanation
arp *<ip_address>* *<mac_address>* {[ethernet] *<portName>*} **no arp *<ip_address>***	Configure a static ARP entry; the "**no arp *<ip_address>*"** command deletes a static ARP entry.

2. Configure proxy ARP

Command	Explanation
ip proxy-arp **no ip proxy-arp**	Enable proxy ARP function for Ethernet ports: the "**no ip proxy-arp"** command disables the proxy ARP. **.**

14.3.2.2 ARP Forwarding Configuration Commands

14.3.2.2.1 Arp

Command: arp <ip_address> <mac_address> {[ethernet] <portName>}
no arp *<ip_address>*

Function: Configure a static ARP entry; the "**no arp *<ip_address>*"** command deletes a static ARP entry.

Parameter: ***<ip_address>*** is the IP address; ***<mac_address>*** is the MAC address; **ethernet** stands for Ethernet port; ***<portName>*** for the name of layer2 port.

Default: No static ARP entry is set by default.

Command mode: VLAN Interface Mode

Usage Guide: Static ARP entries can be configured in the switch.

Example: Configure static ARP for interface VLAN1.
Switch(Config-If-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 eth 1/2

14.3.2.2.2 ip proxy-arp

Command: ip proxy-arp
no ip proxy-arp

Function: Enable proxy ARP for VLAN interface; the **"no ip proxy-arp"** command disables proxy ARP.

Default: Proxy ARP is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: When an ARP request is received on the layer3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, if the interface enabled proxy ARP, the interface would reply to the ARP its own MAC address and forward the actual packets received. Enabling this function allows machines physically separated but of the same IP segment ignores the physical separation and communicates via proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded to if the destination is reachable. Note: ARP request matching default route will not use proxy.

Example: Enable proxy ARP for VLAN 1.
Switch(Config-If-Vlan1)#ip proxy-arp

14.3.3 ARP Forwarding Troubleshooting Help

14.3.3.1 Monitor and Debug Commands

14.3.3.1.1 show arp

Command: show arp [<*ip-addr*>][<*vlan-id*>][<*hw-addr*>][type {static|dynamic}][count] }

Function: Display the ARP table.

Parameter: <*ip-addr*> is a specified IP address; **<*vlan-id*>** stands for the entry for the

identifier of specified VLAN; ***<hw-addr>*** for entry of specified MAC address; “static” for static ARP entry; “dynamic” for dynamic ARP entry; “count” displays number of ARP entries.

Command mode: Admin Mode

Usage Guide: Displays the content of current ARP table such as IP address, MAC address, hardware type and interface name, etc.

Example:

Switch#sh arp

Total arp items: 3, matched: 3, Incomplete: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet3/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet3/4	Dynamic

Displayed information	Explanation
Total arp items	Total number of Arp entries.
the matched	ARP entry number matching the filter conditions.
InCompleted	ARP entries have ARP request sent without ARP reply.
Address	IP address of Arp entries.
Hardware Address	MAC address of Arp entries.
Interface	Layer3 interface corresponding to the ARP entry.
Port	Physical (Layer2) interface corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

14.3.3.1.2 clear arp-cache

Command: clear arp-cache

Function: Clear arp table.

Parameter: N/A.

Command mode: Admin Mode

Usage Guide: Clear the content of current ARP table, but it can’t clear the current static ARP table.

Example:

Switch#clear arp-cache

14.3.3.1.3 debug arp

Command: debug arp

no debug arp

Function: Enable the ARP debug function: the "**no debug arp**" command disables this debug function.

Default: ARP debug is disabled by default.

Command mode: Admin Mode

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enable ARP debug.

Switch#debug arp

ip arp debug is on

Switch#%Apr 19 15: 59: 42 2005 IP ARP: rcvd, type 1, src 192.168.2.100, 000A.EB5B.780C, dst 192.168.2.1, 0000.0000.0000 flag 0x0.

%Apr 19 15: 59: 42 2005 IP ARP: sent, type 2, src 192.168.2.1, 0003.0F02.310A, dst 192.168.2.100, 000A.EB5B.780C.

14.3.3.2 ARP Troubleshooting Help

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP is not learned, then enabled ARP debug information and view sending/receiving condition of ARP packets.
- Defective cable is a common cause of ARP problem and disables ARP learning.

Chapter 15 Routing Protocol Configuration

To communicate with a remote host over the Internet, a host must choose a proper route via a set of routers/L3 switches.

Both routers or layer3 switches calculate the route using CPU, the difference is that layer3 switch adds the calculated route to the switch chip and forward by the chip at wire speed, while the router always store the calculated route in the route table or route buffer, and data forwarding is performed by the CPU. For this reason, although both routers and switches can perform route selection, layer3 switches have a great advantage over routers in data forwarding. ES4626/ES4650 is a layer3 switch.. The following describes basic theory and methods used in layer3 switch route selection.

In route selection, the responsibility of each layer3 switch is to select a proper midway route according to the destination of the packet received; and send the packet to the next layer3 switch until the last layer3 switch in the route sends the packet to the destination host. A route is the path selected by each layer3 switch to pass the packet to the next layer3 switch. Routes can be grouped into direct route, static route and dynamic route.

Direct route refer to the path directly connects to the layer3 switch, and can be obtained with no calculation.

Static route is the manually specified path to a network or a host. Static routes cannot be changed freely. Static routes are simple, consistent, and can limit illegal route modifications, and are convenient for load balancing and route backup. However, as this is set manually, it is not suitable for mid- or large-scale networks for the route in such conditions are too huge and complex.

Dynamic route is the path to a network or a host calculated by the layer3 switch according to the routing protocols enabled. If the next hop layer3 switch in the path is not reachable, layer3 switch will automatically discard the path to that next hop layer3 switch and choose the path through other layer3 switches.

There are two dynamic routing protocols: Interior Gateway Protocol (IGP) and Exterior Gateway protocol (EGP). IGP is the protocol used to calculate the route to a destination inside an autonomous system. IGP supported by ES4626/ES4650 include routing protocols like RIP and OSPF, RIP and OSRF can be configured according to the requirement. ES4626/ES4650 supports running several IGP dynamic routing protocols at the same time. Or, other dynamic routing protocols and static route can be introduced in a dynamic routing protocol, so that multiple routing protocols can be associated.

15.1 Route Table

As mentioned before, layer3 switch is mainly used to establish the route from the current layer3 switch to a network or a host, and to forward packets according to the route. Each

layer3 switch has its own route table containing all routes used by that switch. Each route entry in the route table specifies the VLAN interface should be used for forwarding packet to reach a destination host or the next hop layer3 switch to the host.

The route table mainly consists of the following:

- Destination address: used to identify the destination address or destination network of a packet.
- Network mask: used together with destination address to identify the destination host or the segment the layer3 switch resides. Network mask consists of several consecutive binary 1's, and usually in the format of dotted decimal (an address consists of 1 to 4 255's.) When "AND" the destination address with network mask, we can get the network address for the destination host or the segment the layer3 switch resides. For example, the network address of a host or the segment the layer3 switch resides with a destination address of 200.1.1.1 and mask 255.255.255.0 is 200.1.1.0..
- Output interface: specify the interface of layer3 switch to forward IP packets.
- IP address of the next layer3 switch (next hop): specify the next layer3 switch the IP packet will pass.
- Route entry priority: There may be several different next hop routes leading to the same destination. Those routes may be discovered by different dynamic routing protocols or static routes manually configured. The entry has the highest priority (smallest value) and becomes the current best route. The user can configure several routes of different priority to the same destination; layer3 switch will choose one route for IP packet forwarding according to the priority order.

To avoid too large route table, a default route can be set. Once route table lookup fails, the default route will be chosen for forwarding packets.

The table below describes the routing protocols supported by ES4626/ES4650 and the default route lookup priority value.

Routing Protocols or route type	Default priority value
Direct route	0
OSPF	110
Static route	1
RIP	120
OSPF ASE	150
IBGP	200
EBGP	20
Unknown route	255

15.2 Static Route

15.2.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. Static route is simply and consistent, and can prevent illegal route modification, and is

convenient for load balance and route backup. However, it also has its own defects. Static route, as its name indicates, is static. It won't modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid and large-scale networks.
Static route is mainly used for the following two conditions: 1) in stable networks to reduce load of route selection and routing data streams. For example, static route can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.
Static route and dynamic route can coexist; layer3 switch will choose the route with the highest priority according to the priority of routing protocols. At same time, static route can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced.

15.2.2 Introduction to Default Route

Default route is a static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a packet and has no default route configured, the packet will be dropped, and a ICMP packets will be sent to the source address indicate the destination address or network is unreachable.

15.2.3 Static Route Configuration

15.2.3.1 Static Route Configuration Task Sequence

1. Static Route Configuration
2. Default Route Configuration

1. Static Route Configuration

Command	Explanation
Global Mode	
ip route *<ip_address>* *<mask>* *<gateway>* [*<preference>*] **no ip route *<ip_address>* *<mask>* *<gateway>* [*<preference>*]**	Configures a static route; the "**no ip route *<ip_address>* *<mask>* *<gateway>* [*<preference>*]"** command deletes a static route entry.

2. Default Route Configuration

Command	Explanation
Global Mode	

ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>] **no ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>]**	Configures a default route; the "**no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]"** command deletes a default route entry.

15.2.3.2 Static Route Configuration Commands

- **ip route**
- **show ip route**

15.2.3.2.1 ip route

Command: ip route <ip_address> <mask> <gateway> [<preference>]
no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]

Function: Configures a static route; the "**no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]"** command deletes a static route entry.

Parameter: **<*ip-address*>** and **<*mask*>** are the IP address and subnet mask, in dot decimal format; **<*gateway*>** is the IP address for the next hop in dot decimal format; **<*preference*>** is the route priority, ranging from 1 to 255, the smaller preference indicates higher priority.

Default: The default priority for static route of ES4626/ES4650 is 1.

Command mode: Global Mode

Usage Guide: When configuring the next hop for static route, next hop IP address can be specified for routing packets.

The default preference of all route type in ES4626/ES4650 is listed below:

Route Type	Preference Value
Direct route	0
Static Route	1
OSPF	110
RIP	120
IBEP	200
EBGP	20

By default, direct route has the highest priority, and static route, EBGP, OSPF, RIP and IBGP have descending priorities in the order listed.

Example:

Example 1: add a static route
Switch(Config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1
Example 2: add a default route
Switch(Config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

15.2.3.2.2 show ip route

Command: show ip route [dest <destination>] [mask <destMask>] [nextHop <nextHopValue>] [protocol {connected | static | rip| ospf | ospf_ase | bgp | dvmrp}] [<*vlan-id*>] [preference <*pref*>] [count]

Function: Display the route table.

Parameter: **<*destination*>** is the destination network address; **<*destMask*>** is the mask for destination network; **<*nextHopValue*>** stands for the IP address of next hop; **connected** for direct route; **static** for static route; **rip** for RIP route; **ospf** for OSPF route; **ospf_ase** for route introduced by OSPF; **ospf_asebgp** for BGP route; **bgpdvmrp** for DVMRP route; **<*vlan-id*>** for VLAN identifier; **<*pref*>** for router priority, ranging from 0 to 255; **count** displays the number of IP route table entries.

Command mode: Admin Mode

Usage Guide: Display the content of core route table including: route type, destination network, mask, next hop address, and interface, etc.

Example:

Switch#show ip route

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan2	0
C	4.4.4.0	255.255.255.0	0.0.0.0	vlan4	0
S	6.6.6.0	255.255.255.0	9.9.9.9	vlan9	1
R	7.7.7.0	255.255.255.0	8.8.8.8	vlan8	120

Displayed information	Explanation
C - connected	Direct route, the segment directly connects to the layer3 switch.
S – static	Static route, route are manually configured by the user
R - RIP derived	RIP route, route are obtained through RIP protocol in layer3 switch
O - OSPF derived	OSPF route, route obtained through OSPF protocol in layer3 switch
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, the route obtained through BGP protocol.
Destination	destination network

Mask	Mask of the destination network
Nexthop	Next hop IP address
Interface	The layer3 switch interface to next hop.
Pref	Route priority, if route of the other types exist to the destination network, only the route of the higher priority will be displayed in the core route table.

15.2.4 Configuration Scenario

The figure below is a simple network consisting of three ES4626/ES4650 layer3 switches, the network mask for all switches and PC IP addresses is 255.255.255.0. PC1 and PC3 are connected via the static route set in Swtich1 and Switch3; PC3 and PC2 are connected via the static route set in Swtich3 to Switch2; PC1 and PC3 is connected via the default route set in Switch2.

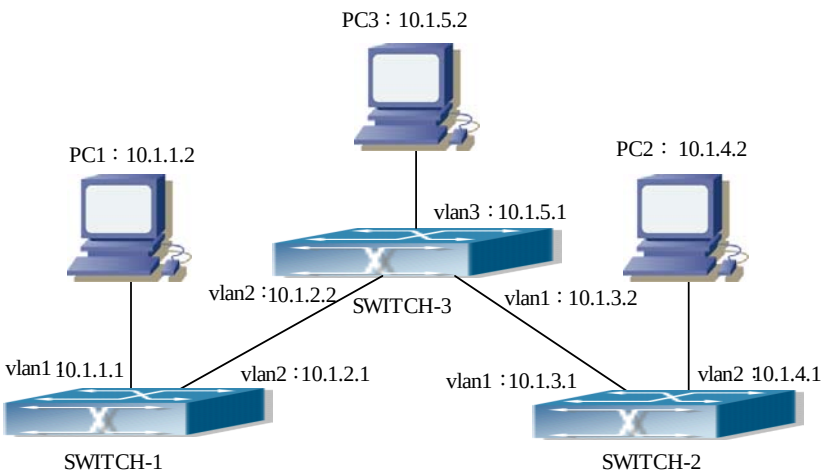


Fig 15-1 Static Route Configurations

Configuration steps:

Configuration of layer3 switch Switch-1

Switch#config

Switch(Config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2

Configuration of layer3 switch Switch-3

Switch#config

！Next hop use the partner IP address

Switch(Config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1

！Next hop use the partner IP address

Switch(Config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1

Configuration of layer3 switch Switch-2

Switch#config

Switch(Config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2

This way, ping connectivity can be established between PC1 and PC3, and PC2 and PC3

15.2.5 Troubleshooting Help

15.2.5.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip route	Displays the content of route table including: route type, destination network, mask, next hop address, and interface, etc.

Use the “show ip route” command to display the information about static route in the route table: destination IP address, network mask, next hop IP address, and forwarding interface, etc.

For example:

Switch#show ip route

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan1	0
S	6.6.6.0	255.255.255.0	2.2.2.9	vlan1	1

S stands for static route, i.e., the static route with the destination network address of 6.6.6.0, network mask of 255.255.255.0, the next hop address of 2.2.2.9 and the forwarding interface of Ethernet vlan1. The priority value of this route is 1.

15.3 RIP

15.3.1 Introduction to RIP

RIP is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIP is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send 2 kind of information to the neighboring devices regularly:

- Number of hops to reach the destination network, or metrics to use or number of networks to pass.
- What is the next hop, or the director (vector) to use to reach the destination network.

Distance vector layer3 switches send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switches will build their own route selecting information table based on the information received from the neighbor layer3 switches. Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, routers beyond 15 hops will be deemed as unreachable.

RIP is a optional routing protocol based on UDP. Hosts using RIP send and receive packets on UDP port 520. All layer3 switches running RIP send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds before deletion.

As layer3 switches running RIP built route table with second hand information, infinite count may occur. For a network running RIP routing protocol, when an RIP route becomes unreachable, the neighboring RIP layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite count” will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To avoid “infinite count”, RIP provides mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately, regardless of the 30 second update timer status.

There two versions of RIP, version 1 and version 2. RFC1058 introduces RIP-I protocol, RFC2453 introduces RIP-II, which is compatible with RFC1723 and RFC1388. RIP-I updates packets by packets advertisement, subnet mask and authentication is not supported. Some fields in the RIP-I packets are not used and are required to be all 0’s; for this reason, such all 0's fields should be checked when using RIP-I, the RIP-I packets should be discarded if such fields are non-zero. RIP-II is a more improved version than RIP-I. RIP-II sends route update packets by multicast packets (multicast address is

224.0.0.9). Subnet mask field and RIP authentication filed (simple plaintext password and MD5 password authentication are supported), and support variable length subnet mask. RIP-II used some of the zero field of RIP-I and require no zero field verification. layer3 switches send RIP-II packets in multicast by default, both RIP-I and RIP-II packets will be accepted.

Each layer3 switch running RIP has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIP layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance. Besides the abovementioned, RIP protocol allows route information discovered by the other routing protocols to be introduced to the route table.

The operation of RIP protocol is shown below:

1. Enable RIP. The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.
2. The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update packet, the neighbor layer 3 switches send triggered update packets to their neighbor layer 3 switches. After a sequence of triggered update packet broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIP layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (holddown timer interval), it will delete that route.

15.3.2 RIP Configuration

15.3.2.1 RIP Configuration Task Sequence

1. Enable RIP (required)
   (1) Enable/disable RIP module.
   (2) Enable interface to send/receive RIP packets
2. Configure RIP parameters (optional)
   (1) Configure RIP sending mechanism
      a Configure specified RIP packets transmission address

b. Configure RIP advertisement

(2) Configure RIP routing parameters.

a. configure route aggregation

b. configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

c. Enable interface to send/receive additional routing metric of RIP packets

d. Configure interface authentication mode and password

(3) Configure other RIP parameters

a. Configure RIP routing priority

b. Configure zero field verification for RIP packets

c. Configure timer for RIP update, timeout and hold-down

3. Configure RIP-I/RIP-II switch

(1) Configure the RIP version to be used in all ports

(2) Configure the RIP version to send/receive in all ports

(3) Configure whether to enable RIP packets sending/receiving for ports

4. Disable RIP

1. Enable RIP

The basic configuration for running RIP on ES4626/ES4650 is quite simple, usually, the user need only enable RIP and enable sending and receiving RIP packets, i.e., send and receive RIP packets according to default RIP configuration (ES4626/ES4650 send RIP-II packets and receive RIP-I/RIP-II packets by default). If necessary, the version of RIP packets to send/receive can be switched, sending/receiving RIP packets can be enabled/disabled, see 3 for details.

Command	Explanation
Global Mode	
[no] router rip	Enables RIP; the "**no router rip**" command disables RIP
Interface Mode	
[no] ip rip work	Enables sending/receiving RIP packets on the interface; the "**no ip rip work**" command disables sending/receiving RIP packets on the interface

2. Configure RIP protocol parameters

(1) Configure RIP sending mechanism

a. Configure regular RIP packets transmission

b. Configure RIP advertisement

Command	Explanation
RIP configuration mode	

[no] rip broadcast	Indicates RIP layer3 switch allow all ports to send broadcast/multicast packets; the "**no rip broadcast**" command disables all ports to send broadcast/multicast packets

2) Configure RIP routing parameters.

a. Configure route aggregation

Command	Explanation
RIP configuration mode	
auto-summary **no auto-summary**	Configures route aggregation; the "**no auto-summary"** command disables route aggregation.

b. configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	Explanation
RIP configuration mode	
default-metric <*value*> **no default-metric**	Sets the default route metric for route to be introduced; the "**no default-metric**" command restores the default setting.
redistribute { static | ospf | bgp} [metric <*value*>] **no redistribute { static | ospf | bgp }**	Introduces static, OSPF or BGP routes to RIP packets; the "**no redistribute { static | ospf | bgp }**" command cancels the introduced routes of specified protocol.

c. Enable interface to send/receive additional routing metric of RIP packets

Command	Explanation
Interface Mode	
ip rip metricout <*value*> **no ip rip metricout**	Sets the additional route metric for route on sending RIP packets from the interface; the "**no ip rip metricout**" command restores the default setting.
ip rip metricin <*value*> **no ip rip metricin**	Sets the additional route metric for route on receiving RIP packets from the interface; the "**no ip rip metricin**" command restores the default setting.

d. Configure interface authentication mode and password

Command	Explanation
Interface Mode	
ip rip authentication mode {text| **md5 type {cisco|usual}}** **no ip rip authentication mode**	Sets the authentication method; the "**no ip rip authentication mode**" command restores the default plain text authentication method.

ip rip authentication key *<name-of-chain>* **no ip rip authentication key**	Sets the authentication key; the "**no ip rip authentication key-chain**" command means no authentication key is used.

3) Configure other RIP parameters

a. Configure RIP routing priority

b. Configure zero field verification for RIP packets

c. Configure timer for RIP update, timeout and hold-down

Command	Explanation
RIP configuration mode	
rip preference *<value>* **no rip preference**	Sets the route priority of RIP; the "**no rip preference**" command restores the default setting.
[no] rip checkzero	Enables zero fields verification to RIP-I packets, refuse to process if non-zero zero field; the "**no rip checkzero**" command cancels this check for zero field
timer basic *<update>* *<invalid>* *<holddown>* **no timer basic**	Adjusts the time of RIP timers for update, expire, and hold down; the "**no timer basic**" command restores the default setting.

3. Configure RIP-I/RIP-II switch

(1) Configure the RIP version to be used in all ports

Command	Explanation
RIP configuration mode	
version { 1 | 2 } **no version**	Sets the version of RIP packets to send/receive on all ports; the "**no version**" command restores the default, i.e., send v2 packets, receive both v1 and v2 packets

(2) Configure the RIP version to send/receive in all ports

(3) Configure whether to enable RIP packets sending/receiving for ports

Command	Explanation
Interface Mode	
ip rip send version { 1 | 2 |v2-broadcast } **no ip rip send version**	Sets the version of RIP packets to send on all ports; the "**no ip rip send version**" command restores the default, i.e., send v2 packets, enables sending RIP packets on the interface.

ip rip receive version {1 | 2 | 1 2} **no ip rip receive version**	Sets the version of RIP packets to receive on all ports; the "**no ip rip receive version**" command restores the default, i.e., receive both v1 and v2 packets, enables receiving RIP packets on the interface.
ip rip receive version none	Disables receiving RIP packets on the interface
ip rip send version none	Disables sending RIP packets on the interface

4. Disable RIP

Command	Explanation
Global Mode	
no router rip	Disables RIP

RIP (Routing Information Protocol) is a dynamic interior routing protocol based on distance vector. It is widely used for its simple configuration. RIP exchanges routing information by UDP packet advertisement, route update information is sent every 30 seconds. It uses hop number to be the standard of choosing route, route of fewer hops to the same destination network will be chosen first. The maximum hop number allowed is 16, so RIP is suitable for autonomous system with relative smaller diameter. RIP configuration commands are mainly used in Global Mode, RIP configuration mode, Interface Mode and Admin Mode.

15.3.2.2 RIP Configuration Commands

- **auto-summary**
- **default-metric**
- **ip rip authentication key**
- **ip rip authentication mode**
- **ip rip metricin**
- **ip rip metricout**
- **ip rip receive version**
- **ip rip receive version none**
- **ip rip send version**
- **ip rip send version none**
- **ip rip work**
- **ip split horizon**
- **redistribute**
- **rip broadcast**
- **rip checkzero**
- **rip preference**

- **router rip**
- **timer basic**
- **version**
- **show ip protocols**
- **show ip rip**
- **debug ip rip packet**
- **debug ip rip recv**
- **debug ip rip send**

15.3.2.2.1 auto-summary

Command: auto-summary
no auto-summary
Function: Configure route aggregation; the "**no auto-summary"** command disables route aggregation.
Parameter: N/A.
Default: Auto route aggregation is not used by default.
Command mode: RIP configuration mode
Usage Guide: Route aggregation reduces the amount of routing information in the route table and amount of information to be exchanged. RIP-I does not support subnet mask, forwarding subnet route may result in ambiguity. For this reason, route aggregation is always enabled for RIP-I. If you are using RIP-II, you can use "no auto-summary" command to disable route aggregation. If subnet route needs to be broadcasted, route aggregation can also be disabled.
Example: Set the RIP version to RIP-II and disables route aggregation.
Switch(Config)#router rip
Switch(Config-Router-Rip)#version 2
Switch(Config-Router-Rip)#no auto-summary
Related command: version

15.3.2.2.2 default-metric

Command: default-metric <*value*>
no default-metric
Function: Set the default route metric for route to be introduced; the "**no default-metric**" command restores the default setting.
Parameter: < *value*> is the value of route metric, ranging from 1 to 16.
Default: The default route metric is 1.
Command mode: RIP configuration mode
Usage Guide: "**default-metric**" command sets the default route metric used in

introducing routes from the other routing protocols to RIP. When using "**redistribute**" command to introduce routes of the other protocols without specifying detailed route metric, the default route metric set by "**default-metric**" command applies.

Example: Set the default route metric for introducing routes of the other protocols into RIP to 3.

Switch(Config-router-rip)#default-metric 3

Related command: redistribute

15.3.2.2.3 ip rip authentication key

Command: ip rip authentication key <*name-of- key* >

no ip rip authentication key

Function: Specify the key to use for RIP authentication; the "**no ip rip authentication key-chain**" command cancels the RIP authentication.

Parameter: <*name-of- key* > is a string, up to 16 characters are allowed.

Default: RIP authentication is disabled by default.

Command mode: Interface Mode

Usage Guide: Instead of deleting the RIP authentication key, the "**no ip rip authentication key-chain**" command cancels the RIP authentication.

Related command: ip rip authentication

15.3.2.2.4 ip rip authentication mode

Command: ip rip authentiaction mode {text|md5 type {cisco|usual}}

no ip rip authentication mode

Function: Set the authentication method; the "**no ip rip authentication mode**" command restores the default plain text authentication method.

Parameter: "**text**" for text authentication; "**md5**" for MD5 authentication. There two MD5 authentication methods, Cisco MD5 and conventional MD5.

Default: The default setting is text authentication.

Command mode: Interface Mode

Usage Guide: RIP-I does not support authentication, RIP-II support 2 authentication methods: text authentication (Simple authentication) and packets authentication (MD5 authentication). There 2 packets types used in MD5 authentication, one format complies with RFC1723 (RIP Version 2 Carrying Additional Information), the other format conforms to RFC2082 (RIP-II MD5 Authentication).

Example: Set Cisco MD5 authentication on interface vlan1, the authentication key is "switch".

Switch(Config-If-Vlan1)#ip rip authentication mode md5 type cisco

Switch(Config-If-Vlan1)#ip rip authentication key switch

Related command: ip rip authentication key

15.3.2.2.5 ip rip metricin

Command: ip rip metricin <*value*>
no ip rip metricin
Function: Set the additional route metric receiving RIP packets on the interface; the "**no ip rip metricin**" command restores the default setting.
Parameter: < *value*> is the additional route metric, ranging from 1 to 15.
Default: The default additional route metric used for RIP to receive packets is 1.
Command mode: Interface Mode
Related command: ip rip metricout

15.3.2.2.6 ip rip metricout

Command: ip rip metricout <*value*>
no ip rip metricout
Function: Set the additional route weight sending RIP packets on the interface; the "**no ip rip metricout**" command restores the default setting.
Parameter: < *value*> is the additional route metric, ranging from 0 to 15.
Default: The default additional route metric used for RIP to send packets is 0.
Command mode: Interface Mode
Example: Set on interface vlan1 the additional route metric of receiving RIP packets to 5, and sending RIP packets to 3.
Switch(Config-If-Vlan1)#ip rip metricin 5
Switch(Config-If-Vlan1)#ip rip metricout 3
Related command: ip rip metricin

15.3.2.2.7 ip rip receive version none

Command: ip rip receive version none
Function: Disable receiving RIP packets on the interface; the "**no ip rip input**" command disables receiving RIP packets on the interface
Default: Receiving RIP packet is enabled by default.
Command mode: Interface Mode
Usage Guide: This command is used with the other two commands "**no ip rip receive version**" and "**ip rip work**", "**ip rip work**" is equal to "**no ip rip receive version** & **no ip rip send version**" in function, the latter two commands control the receiving and sending of RIP packet on the interface, the former equals the total of the latter two commands.

Related command: no ip rip send version

15.3.2.2.8 ip rip send version none

Command: ip rip send version none
Function: Disable sending RIP packets on the interface
Default: Sending RIP packet is enabled by default.

Command mode: Interface Mode
Usage Guide: This command is used with the other two commands "**ip rip output**" and "**ip rip work**", "**ip rip work**" is equal to "**ip rip input**" & "**ip rip output**" in function, the latter two commands control the receiving and sending of RIP packet on the interface, the former equals the total of the latter two commands.

Related command: no ip rip send version

15.3.2.2.9 ip rip receive version

Command: ip rip receive version {1 | 2 | 1 2}
no ip rip receive version
Function: Configure RIP version to receive on the interface. The default setting is to receive both RIP v1 and v2 packets; the "**no ip rip receive version**" command restores the default setting, enables receiving RIP packets on the interface.
Parameter: 1 and **2** stands for RIP version1 and RIP version 2 respectively, **12** stands for both RIP version 1 and 2.
Default: The default setting is **12**, i.e., accept both RIP version 1 and version 2 packets.
Command mode: Interface Mode

15.3.2.2.10 ip rip send version

Command: ip rip send version { 1 | 2 | v2-broadcast }
no ip rip send version
Function: Configure RIP version to send on the interface; the "**no ip rip send version**" command restores the default setting, enables sending RIP packets on the interface.
Parameter: 1 | 2 are both RIP version numbers; **v2-broadcast** is broadcast only for RIP-II. When configured to send RIP-II packets, the interface sends RIP-II packets in multicast by default, packets are only broadcasted when **v2-broadcast** is set on the interface.
Default: RIP-II packets are sent by default.

Command mode: Interface Mode
Usage Guide: When configured to send RIP-II packets, the interface sends RIP-II packets

in multicast by default, packets are only broadcasted when **v2-broadcast** is set on the interface.

15.3.2.2.11 ip rip work

Command: ip rip work
no ip rip work
Function: Configure the interface to run RIP or not; the "**no ip rip work**" command disables RIP packet sending/receiving on the interface.
Default: After enabling RIP, RIP is enabled on the ports by default.
Command mode: Interface Mode
Usage Guide: This command is equal to "**no ip rip send version** & **no ip rip receive version**" in function, the latter two commands control the receiving and sending of RIP packet on the interface, the former equals the total of the latter two commands.
Related command: no ip rip send version 、no ip rip receive version

15.3.2.2.12 ip split-horizon

Command: ip split-horizon
no ip split-horizon
Function: Set to enable split horizon; the "**no ip split-horizon**" command disables split horizon.
Default: split horizon is enabled by default.
Command mode: Interface Mode
Usage Guide: Set split horizon to prevent routing loops, i.e. prevent layer3 switch from broadcasting the route leaned from the same interface.
Example: Disable split horizon for interface vlan1.
Switch(Config)#interface vlan1
Switch(Config-If-Vlan1)#no ip split-horizon

15.3.2.2.13 redistribute

Command: redistribute { static | ospf | bgp} [metric <*value*>]
no redistribute { static | ospf | bgp }
Function: Introduce routes of the other protocols into RIP; the "**no redistribute { static | ospf | bgp }**" command cancels the introduction.
Parameter: static specifies static routes to be introduced; **ospf** for OSPF routes; **bgp** for BGP routes; **<*value*>** stands for the route metric in introducing the routes, ranging from 1 to 16.

Default: Other routes are not introduced to RIP by default. If routes of the other routing protocols are introduced without metric value, the default metric value is used.

Command mode: RIP configuration Mode

Usage Guide: Use this command to introduce routes of the other routing protocols as RIP route to improve RIP performance.

Example: Set on the route metric of OSPF route to 5, and static route metric to 8.

Switch(Config-Router-Rip)#redistribute ospf metric 5

Switch(Config-Router-Rip)#redistribute static metric 8

15.3.2.2.14 rip broadcast

Command: rip broadcast

no rip broadcast

Function: Configure RIP layer3 switch allow all ports to send broadcast/multicast packets; the "**no rip broadcast**" command disables all ports to send broadcast/multicast packets, instead, only neighbor layer3 switches can exchange RIP packets.

Default: RIP broadcast packets are sent by default.

Command mode: RIP configuration Mode

15.3.2.2.15 rip checkzero

Command: rip checkzero

no rip checkzero

Function: Use this command to check the zero fields of RIP-I packets, the "**no rip checkzero**" command cancel this check for zero field. Since there are no zero fields in RIP-II packets, this command has no effect on RIP-II packets.

Default: Zero field check for RIP-I packets is performed by default.

Command mode: RIP configuration mode

Usage Guide: RIP-I packet must have zero field, this command can be used to enable/disable check for RIP-I packet zero field. If non-zero zero field found in RIP-I packet, that RIP-I packet will be discarded.

Example: Disable zero field check for RIP-I packets.

Switch(Config-router-rip)#no ip checkzero

15.3.2.2.16 rip preference

Command: rip preference <*value*>

no rip preference

Function: Set the route priority of RIP; the "**no rip preference**" command restores the default setting.

Parameter: < *value*> is the priority value, ranging from 0 to 255.

Default: The default RIP priority is 120.

Command mode: RIP configuration mode

Usage Guide: Each routing protocol has its own priority, the value of which is decided by the specific routing policy. The priority determines the best route of what routing protocol will be the route in the core route table. This command can be used to manually adjust RIP priority; the adjustment will apply to new routes. Due to the nature of RIP, the RIP priority should not be set too high.

Example: Set the RIP priority to 10.

Switch(Config-router-rip)#rip prefenrence 10

15.3.2.2.17 router rip

Command: router rip

no router rip

Function: Enable RIP and enter RIP configuration mode; the "**no router rip**" command disables RIP.

Default: RIP is disabled by default.

Command mode: Global Mode

Usage Guide: This command is the enabling switch for RIP, it must be run before other configurations to RIP can be made.

Example: Enable RIP configuration mode

Switch(Config)#router rip

Switch(Config-Router-Rip)#

15.3.2.2.18 timer basic

Command: timer basic <update> <invalid> <holddown>

no timer basic

Function: Adjust the time of RIP timers for update, expire, and hold down; the "**no timer basic**" command restores the default setting.

Parameter <*update*> stands for the interval in seconds to send update packets, ranging from 1 to 2,147,483,647; ***<invalid>*** for the interval in seconds to declare a RIP route invalid, ranging from 1 to 2,147,483,647; ***<holddown>*** for the interval in seconds to keep a RIP route after it is declared to be invalid, ranging from 1 to 2,147,483,647.

Default: The default value for ***<update>*** is 30; 180 for ***<invalid>***; and 120 for <***holddown***>.

Command mode: RIP configuration mode

Usage Guide: The system advertises RIP update packets every 30 seconds by default. If no update packet form a route is received after 180 seconds, this route is considered to be invalid. However, the route will be kept in the route table for another 120 seconds, and will be deleted after that. It should be noted in adjusting RIP timeout timers that the time to declare invalid route should be at least greater than RIP update time, holddown time should also be greater than RIP update interval and must be integer multiples of the RIP update interval.

Example: Set the RIP route table update time to 20 seconds, time to declare invalid to 80 seconds, and time to delete entry to 60 seconds.

Switch(Config-Router-Rip)#timer basic 20 80 60

15.3.2.2.19 version

Command: version {1| 2}

no version

Function: Configure the RIP version to send/receive on all ports; the "**no version**" command restores the default setting.

Parameter: 1 for RIP version 1, 2 for RIP version 2.

Default: The default setting sends RIP-I packets and receives both RIP-I and RIP-II packets.

Command mode: RIP configuration mode

Usage Guide: 1 means all ports only send/accept RIP-I packets, 2 for send/accept RIP-II packets only. The default setting sends RIP-I packets and receives both RIP-I and RIP-II packets.

Example: Set the interface to send/receive RIP-II packets.

Switch(Config-router-rip)#version 2

Related command: ip rip receive version

ip rip send version

15.3.2.2.20 show ip protocols

Command: show ip protocols

Function: Display the information of the routing protocols running in the switch.

Command mode: Admin Mode

Usage Guide: The user can decide whether the routing protocols configured are correct

and perform routing troubleshooting according to the output of this command.

Example:

Switch#sh ip protocols

RIP information

rip is turning on

default metrict 16

neighbour is: NULL

preference is 100

rip version information is:

interface	send version	receive version
vlan2	V2BC	V12
vlan3	V2BC	V12
vlan4	**V2BC**	**V12**

Displayed information	Explanation
RIP is turning on	The running routing protocol is RIP.
default metric	RIP protocol default metric value.
neighbour is:	The neighbor layer3 switch connecting to this RIP switch.
Preference	RIP routing priority.
rip version information	Display the version information for RIP, including the RIP version of sending (V1 for RIP-I, V2 for RIP-II), RIP sending method (BC for broadcast, MC for multicast), RIP version of receiving (V1 for RIP-I, V2 for RIP-II, V12 for both RIP-I and RIP-II).

15.3.2.2.21 show ip rip

Command: show ip rip

Function: Display the current running status and configuration information for RIP.

Command mode: Admin Mode

Usage Guide: The user can check the default metric of RIP route, the specified sending destination address and metric value according to the output of this command.

Example:

Switch#sh ip rip

RIP information
rip is turning on
default metric 16
neighbour is
preference is 100

Displayed information	Explanation
rip is turning on	RIP routing is enabled
default metric 16	The default metric for introduced route is 16.
neighbour is	The specified destination address.
preference is 100	RIP routing priority is 100.

15.3.2.2.22 debug ip rip packet

Command: debug ip rip packet
no debug ip rip packet
Function: Enable the RIP packet debug function for sending/receiving: the “no debug IP packet” command disables this debug function.
Default: Debug is disabled by default.
Command mode: Admin Mode
Example:
Switch#debug ip rip pa
"debug ip rip pa" executed successfully.
00: 04: 20:

start at 260**********
send packets to 11.11.11.2
packet header: cmd: response, version: 1
no. dest dest_mask gatedway metric
1: 159.226.0.0 0.0.0.0 0.0.0.0 1
00: 04: 20:

start at 260**********
send packets to 159.226.255.255
packet header: cmd: response, version: 1
no. dest dest_mask gatedway metric
1: 159.222.0.0 0.0.0.0 0.0.0.0 2

2: 11.11.11.2 0.0.0.0 0.0.0.0 2
00: 04: 20:

start at 260**********
received a rip packet from 159.226.42.1
rip packet cmd : 2 version: 1

15.3.2.2.23 debug ip rip recv

Command: debug ip rip recv
no debug ip rip recv
Function: Enable the RIP packet debug function for receiving: the "**no debug ip rip recv**" command disables the debug function.
Default: Debug is disabled by default.
Command mode: Admin Mode
Example:
Switch#debug ip rip rec

start at 230**********
received a rip packet from 159.226.42.1
rip packet cmd : 2 version: 1
00: 03: 59:

start at 238**********
received a rip packet from 11.11.11.2
rip packet cmd : 2 version: 1
00: 03: 59:
rip receive response
packet head 14872964; packet end 14872984
recv packets from 11.11.11.2
packet header: cmd: response, version: 1
no. dest dest_mask gatedway metric
1: 159.222.0.0 0.0.0.0 0.0.0.0 1

15.3.2.2.24 debug ip rip send

Command: debug ip rip send
no debug ip rip send

Function: Enable the RIP packet debug function for sending: the "**no debug ip rip send**" command disables the debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

Example:

```
Switch#debug ip rip send
00: 02: 50:
 start at 170**********************
send packets to          11.11.11.2
packet header:   cmd: response, version: 1
no.        dest                dest_mask          gatedway   metric
1:       159.226.0.0          0.0.0.0            0.0.0.0       1
00: 02: 50:
start at 170**********************
send packets to   159.226.255.255
packet header:   cmd: response, version: 1
no.        dest                dest_mask          gatedway   metric
1:         159.222.0.0          0.0.0.0            0.0.0.0     2
2:          11.11.11.2          0.0.0.0            0.0.0.0     2
```

15.3.3 Typical RIP Scenario

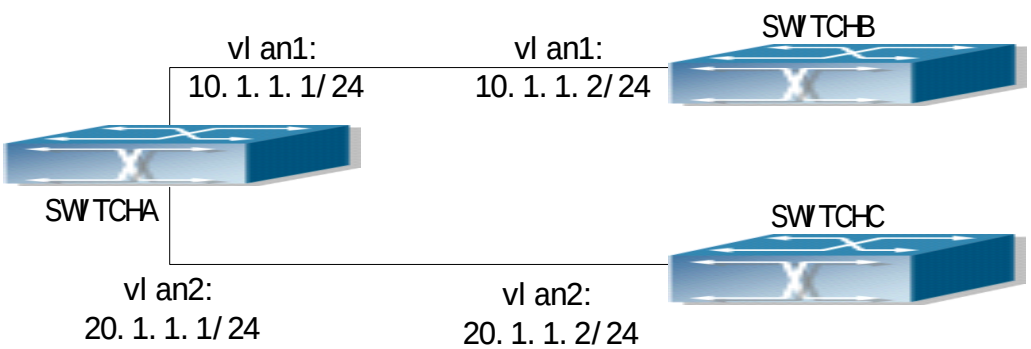


Fig 15-2 RIP Scenario

As shown in the figure a network consists of three layer 3 switches. SwitchA and SwitchB connect to SwitchC through interface vlan1 and vlan2. All the three switches are running RIP. Assume SwitchA vlan1(10.1.1.1) and vlan2 (20.1.1.1) exchange update information with SwitchB vlan1 (10.1.1.2) only, update information is not exchanged between switchA and switchC vlan2 (20.1.1.2).

The configuration for SwitchA, SwitchB and SwitchC is shown below:

a) Configuration of layer3 switch SwitchA

```
!Configuration of the IP address for interface vlan1
SwitchA#config
SwitchA(Config)# interface vlan 1
SwitchA(Config-If-Vlan1)# ip address 10.1.1.1 255.255.255.0
SwitchA (Config-If-vlan1)#exit
!Configuration of the IP address for interface vlan2
SwitchA(Config)# interface vlan 2
SwitchA(Config-If-vlan2)# ip address 20.1.1.1 255.255.255.0
！Enable RIP
SwitchA(Config)#router rip
SwitchA(Config-router-rip)#exit
！Enable vlan1 to send/receive RIP packets
SwitchA(Config)#interface vlan 1
SwitchA(Config-If-vlan1)#ip rip work
SwitchA(Config-If-vlan1)#exit
！Enable vlan2 to send/receive RIP packets
SwitchA (Config-If-vlan2)# ip rip work
SwitchA (Config-If-vlan2)#exit
SwitchA(Config)#exit
SwitchA#
```

b) Configuration of layer3 switch SwitchB

```
!Configuration of the IP address for interface vlan1
SwitchB#config
SwitchB(Config)# interface vlan 1
SwitchB(Config-If-vlan1)# ip address 10.1.1.2 255.255.255.0
SwitchB (Config-If-vlan1)exit
！Enable RIP and configure the IP address for the neighbor layer3 switch
SwitchB(Config)#router rip
SwitchB(Config-router-rip)#exit
！Enable vlan1 to send/receive RIP packets
SwitchB(Config)#interface vlan 1
SwitchB (Config-If-vlan1)#ip rip work
SwitchB (Config-If-vlan1)#exit
SwitchB(Config)#exit
SwitchB#
```

c) Configuration of layer3 switch SwitchC

```
!Configuration of the IP address for interface vlan2
SwitchC#config
```

```
SwitchC(Config)# interface vlan 2
SwitchC(Config-If-vlan2)# ip address 20.1.1.2 255.255.255.0
SwitchC (c config-If-vlan2)#exit
！Enable RIP
SwitchC(Config)#router rip
SwitchC(Config-router-rip)#exit
！Enable vlan2 to send/receive RIP packets
SwitchC(Config)#interface vlan 2
SwitchC (Config-If-vlan2)#ip rip work
SwitchC (Config-If-vlan2)exit
SwitchC(Config)#exit
SwitchC#
```

15.3.4 RIP Troubleshooting Help

1. Monitor and Debug Commands
2. RIP Troubleshooting Help

15.3.4.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip rip	Display the current running status and configuration information for RIP. The user can decide whether the configurations are correct or not and perform RIP troubleshooting according to the output of this command.
show ip route	Display route table information, RIP routing information can be checked.
show ip protocols	Displayed protocol information
[no] debug ip rip packet	Display all RIP packets received and sent.
[no] debug ip rip recv	Display all RIP packets received
[no] debug ip rip send	Display all RIP packets sent.

（1）show ip rip

Displayed information:

RIP information:

Automatic network summarization is not in effect.

default metric for redistribute is : 16

neigbour is : NULL

preference is : 100

Explanation to displayed information:

Displayed information	Explanation
Automatic network summarization is not in effect	Disable RIP auto aggregation
default metric for redistribute is : 16	The default metric for introduced route is 16.
neigbour is	The specified destination address.
preference is : 100	RIP routing priority is 100.

（2）show ip route

The “show ip route” command can be used to display the information about RIP routes in the route table: destination IP addresses, network masks, next hop IP addresses, and forwarding interfaces, etc.

For example, displayed information can be:

Switch#show ip route

Total route items is 2, the matched route items is 2

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived, D - DVMRP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan1	0
R	7.7.7.0	255.255.255.0	2.2.2.8	vlan2	100

R stands for RIP route, i.e., the RIP route with the destination network address of 7.7.7.0, network mask of 255.255.255.0, the next hop address of 2.2.2.8 and the forwarding interface of Ethernet vlan2. The priority value of this route is 100.

（3）show ip protocols

“show ip protocols” command can be used to display the information of the routing protocols running in the switch.

For example, displayed information can be:

Switch#sh ip protocols

RIP information:

Automatic network summarization is not in effect.

default metric for redistribute is : 16

neigbour is: NULL

preference is : 100

RIP version information is:

interface	send version	receive version
vlan1	V2BC	V12
vlan2	V2BC	V12
vlan3	V2BC	V12

Switch#

Displayed information	Explanation
Automatic network summarization is not in effect	Disable RIP auto aggregation
default metric for redistribute is :	RIP protocol default metric value.
neigbour is:	The neighbor layer3 switch connecting to this RIP switch.
Preference	RIP routing priority.
RIP version information	Display the version information for RIP, including the RIP version of sending (V1 for RIP-I, V2 for RIP-II), RIP sending method (BC for broadcast, MC for multicast), RIP version of receiving (V1 for RIP-I, V2 for RIP-II, V12 for both RIP-I and RIP-II).

15.3.4.2 RIP Troubleshooting Help

In configuring and using RIP, the RIP may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interface status” command).
- ✧ Enable RIP (use “router rip” command) first, then configure RIP parameters in the appropriate ports, such as use RIP-I or RIP-II.
- ✧ Next, note the inherent nature of RIP: RIP layer3 switch send route table update information to all its neighbor layer3 switches every 30 seconds, if information from a certain layer3 switch is not received in 180 seconds, that switch is considered failed or unreachable, the route of that switch will be kept in the route table for another 120 seconds before deleting. As a result, if a RIP route is deleted, wait 300 seconds to ensure the entry to be removed from the route table.

15.4 OSPF

15.4.1 Introduction to OSPF

OSPF is short for Open Shortest Path First. It is an interior dynamic routing protocol for autonomous system based on link-state. The protocol creates a link-state database by exchanging link-state among layer3 switches, and then uses the Open Shortest Path First

algorithm to generate a route table based on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other host on the Internet are not managed by those AS and they don't share interior routing information with the layer3 switches on the Internet.

Each link-state layer3 switches can provide information about the topology with its neighboring layer3 switches.

- The segment (link) connecting to the layer3 switches
- State of the connecting link

Link-state information is flooded throughout the network so that all layer3 switches can get firsthand information. Link-state layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state layer3 switches establish neighborhood by sending "HELLO" to their neighbors, then link-state advertisements (LSA) will be sent among neighboring layer3 switches. Neighboring layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as "flooding". In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packets to pass, link bandwidth, current load of the link, and can even add metric by the administrator for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO packet to get to know its neighbors and establish neighborhood.

2) The neighbors respond with information about the link they are connecting and the related costs.

3) The originate layer3 switch uses this information to build its own routing table.

4) Then, as part of the regular update, layer3 switch send link-state advertisement (LSA) packets to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.

5) Each neighboring layer3 switch copies the LSA packet and passes it to the next neighbor (flooding).

6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is, converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages released some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPF protocol include the following. OSPF supports networks of various scales; several hundreds of layer3 switches can be supported in a OSPF network. Routing topology change can be quickly found and converged. Link-state information is used in shortest path algorithm for route calculation, eliminating endless loop. OSPF divides the autonomous system intro ***areas***, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the

autonomous system, they can be grouped as internal switches, edge switches, AS edge switches and backbone switches). OSPF supports load balance and multiple routes to the same destination of equal costs. OSPF supports 4 level routing mechanisms (process routing according to the order of route inside an area, route between areas, first category exterior route and second category exterior route). OSPF support IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPF supports sending packets in multicast.

Each OSPF layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with the other OSPF layer3 switches to formal a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted in itself according to the link-state database, this tree provide the route to all nodes in an autonomous system. If 2 or more layer3 switches exist (multi-access to the network), "designated layer3 switch" and "backup designated layer3 switch" will be selected. Designated layer3 switch is responsible for broadcasting link-state of the network. This concept helps the traffic among the switches.

OSPF protocol requires the autonomous system to be divided into areas. That is to divide the

autonomous system into 0 field (back field) and non-0 filed. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPF uses four different kinds of routes; they are the route inside the area, route between areas, first category exterior route and second category exterior route, in the order of highest priority to lowest. The route inside an area and between areas describe the internal network structure of an autonomous system, while external routes describe the routing information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, the costs of those routes are fair to the costs of OSPF routes; the second type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, but the costs of those routes are far greater than that of OSPF routes, and OSPF route cost is ignored when calculating route costs.

OSPF areas are centered with the Backbone area, identified as the 0 area, all the other areas must be connected to the 0 area logically, and the 0 area must be online. For this reason, the concept of virtual connection is introduced to the backbone area, so that physically separated areas still have logical connectivity to this area. The configurations of all the layer3 switches in the same area must be the same.

In conclusion, LSA can only be transferred between neighboring layer3 switches, OSPF protocol includes 5 types of LSA: router LSA, network LSA, summary LSA to the other areas, general LSA to AS edge switches and exterior AS LSA. They can also be called type1 LSA, type2 LSA, type3 LSA, type4 LSA, and type5 LSA. Router LSA is generated by each layer3 switch inside an OSPF area, and is sent to all the other neighboring layer3 switches; network LSA is generated by the specified layer3 switch in the OSPF area of multi-access network, and is sent to all the other neighboring layer3 switches. (In order to reduce traffic on layer3 switches in the multi-access network, "designated layer3 switch" and "backup designated layer3 switch" should be selected in the multi-access network, and the network link-state is broadcasted by the designated layer3 switch); summary LSA is generated by switches in OSPF area edge, and is transferred among area edge layer3 switches; AS exterior LSA is generated by layer3 switches on exterior edge of AS, and is transferred throughout the AS.

As to autonomous systems mainly advertises exterior link-state, OSPF allow some areas

to be configured as STUB areas to reduce the topology database size. Type4 LSA (ASBR summary LSA) and type5 LSA (AS exterior LSA) are not allowed to flood into/through STUB areas. STUB areas must use the default routes, the layer3 switches on STUB area edge advertise the default routes to STUB areas by summary LSA, those default routes flood inside STUB only and will not get out of STUB area. Each STUB area has a corresponding default route, the route from a STUB area to AS exterior destination must rely on the defaulted route of that area.

The following outlines OSPF priority route calculation process:

1） Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to the other layer3 switches through link-state update (LSU) packets. This way, each layer3 switch receives LSAs from the other layer3 switches, and all LSAs combined to the link-state database.

2） Since an LSA is a description to the network topology structure around a layer3 switch, the LS database is the description to the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.

3） Each layer3 switch uses the shortest path finding (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPF protocol is developed by the IETF, the OSPF v2 widely used now is fulfilled according to the content described in RFC2328.

15.4.2 OSPF Configuration

The OSPF configuration for the series switches may be different from the configuration procedure to switches of the other manufacturers. It is a two-step process:

1. Enable OSPF in the Global Mode;
2. Configure OSPF area for the interface.

15.4.2.1 Configuration Task Sequence

1. Enable OSPF (required)
   (1) Enable/disable OSPF (required)
   (2) Configure the ID number of the layer3 switch running OSPF (optional)
   (3) Configure the network scope for running OSPF (optional)
   (4) Configure the area for the interface (required)
2. Configure OSPF sub-parameters (optional)

(1) Configure OSPF packet sending mechanism parameters

a. Configure OSPF packet verification

b. Set the OSPF interface to receive only

c. Configure the cost for sending packets from the interface

d. Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

(2) Configure OSPF route introduction parameters

a. Configure default parameters (default type, default tag value, default cost, default interval and default number uplimit)

b. Configure the routes of the other protocols to introduce to OSPF.

(3) Configure other OSPF protocol parameters

a. Configure OSPF routing protocol priority

b. Configure cost for OSPF STUB area and default route

c. Configure OSPF virtual link

d. Configure the priority of the interface when electing designated layer3 switch (DR).

3. Disable OSPF protocol.

1. Enable OSPF protocol

Basic configuration of OSPF routing protocol on route switch is quite simple, usually only enabling OSPF and configuration of the OSPF area for the interface are required. The OSPF protocol parameters can use the default settings. If OSPF protocol parameters need to be modified, please refer to “2. Configure OSPF sub-parameters”.

Command	Explanation
Global Mode	
[no] router ospf	Enables OSPF protocol; the “**no router ospf**” command disables OSPF protocol (required)

router id <*router_id*> **no router id**	Configures the ID number for the layer3 switch running OSPF; the “**no router id**” command cancels the ID number. The IP address of an interface is selected to be the layer3 switch ID. (optional)
OSPF protocol configuration mode	
[no] network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]	Defines several segments in an area to a network scope; the “**no network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]**” command cancels the network scope. (optional)
Interface Mode	

ip ospf enable area <*area_id*> **no ip ospf enable area**	Sets an area for the specified interface; the "**no ip ospf enable area**" command cancels the setting. (required)

2. Configure OSPF sub-parameters

(1) Configure OSPF packet sending mechanism parameters

a. Configure OSPF packet verification

b. Set the OSPF interface to receive only

c. Configure the cost for sending packets from the interface

Command	Explanation
Interface Mode	
ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>} **no ip ospf authentication**	Configures the authentication method and key required by the interface to accept OSPF packets; the "**no ip ospf authentication**" command restores the default setting.
[no] ip ospf passive-interface	Sets an interface to receive only, the "no **ip ospf passive-interface"** command cancels the setting.
ip ospf cost <*cost* > **no ip ospf cost**	Sets the cost for running OSPF on the interface; the "**no ip ospf cost**" command restores the default setting.

d. Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

Command	Explanation
Interface Mode	
ip ospf hello-interval <*time*> **no ip ospf hello-interval**	Sets interval for sending HELLO packets; the "**no ip ospf hello-interval**" command restores the default setting.
	This line should be deleted.
ip ospf dead-interval <*time* > **no ip ospf dead-interval**	Sets the interval before regarding a neighbor layer3 switch invalid; the "**no ip ospf dead-interval**" command restores the default setting.
ip ospf transmit-delay <*time*> **no ip ospf transmit-delay**	Sets the delay time before sending link-state broadcast; the "**no ip ospf transmit-delay**" command restores the default setting.
ip ospf retransmit <*time*> **no ip ospf retransmit**	Sets the interval for retransmission of link-state advertisement among neighbor layer3 switches; the "**no ip ospf retransmit**" command restores the default setting.

(2) Configure OSPF route introduction parameters

a. Configure default parameters (default type, default tag value, default cost, default interval and default number uplimit)

Command	Explanation
OSPF protocol configuration mode	
default redistribute type { 1 | 2 } **no default redistribute type**	Sets the default route weight for route to be introduced; the "**no default-metric**" command restores the default setting.

default redistribute tag <*tag*> **no default redistribute tag**	Sets the default tag value for introducing external routes; the "**no default redistribute tag**" command cancels the tag value setting.
default redistribute cost <*cost*> **no default redistribute cost**	Sets the default cost for introducing external routes; the "**no default redistribute cost**" command cancels the cost for introducing external routes. .
default redistribute interval <*time*> **no default redistribute interval**	Sets the interval for introducing external routes; the "**no default redistribute interval**" command restores the default setting.
default redistribute limit <*routes*> **no default redistribute limit**	Sets the uplimit for external routes introduction; the "**no default redistribute limit**" command restores the default setting.

b. Configure the routes of the other protocols to introduce to OSPF.

Command	Explanation
OSPF protocol configuration mode	
redistribute ospfase { bgp | connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>] **no redistribute ospfase { bgp | connected | static | rip }**	Introduces BGP routes, direct routes, static routes and RIP routes as external routing information; the "no redistribute ospfase { bgp | connected | static | rip }" command cancels the introduction of external routing information.

(3) Configure other OSPF protocol parameters

a. Configure OSPF routing protocol priority

b. Configure cost for OSPF STUB area and default route

c. Configure OSPF virtual link

Command	Explanation
OSPF protocol configuration mode	
preference [ase] <*preference* > **no preference [ase]**	Configures the priority of OSPF among all the routing protocols, and the priority for AS exterior routes introduced; the "**no preference [ase]**" command restores the default setting.
stub cost <*cost*> area <*area_id* > **no stub area <area_id >**	Sets an area to STUB area; the "**no stub area <area_id >"** command cancels the setting.

virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit <*time*>] [transitdelay <*time*>] **no virtuallink neighborid <*router_id*> transitarea <*area_id*>**	Creates and configures virtual link; the "**no virtuallink neighborid <*router_id*> transitarea <*area_id*>**" command deletes a virtual link.

d. Configure the priority of the interface when electing designated layer3 switch (DR).

Command	Explanation
Interface Mode	
ip ospf priority <*priority*> **no ip ospf priority**	Sets the priority of the interface in "designated layer3 switch" election; the "**no ip ospf priority**" command restores the default setting.

3. Disable OSPF protocol.

Command	Explanation
Global Mode	
no router ospf	Disables OSPF routing protocol

15.4.2.2 OSPF Configuration Commands

- **default redistribute cost**
- **default redistribute interval**
- **default redistribute limit**
- **default redistribute tag**
- **default redistribute type**
- **ip opsf authentication**
- **ip ospf cost**
- **ip opsf dead-interval**
- **ip ospf enable area**
- **ip ospf hello-interval**
- **ip ospf passive-interface**
- **ip ospf priority**
- **ip ospf retransmit-interval**
- **ip ospf transmit-delay**
- **network**
- **preference**
- **redistribute ospfase**
- **router id**

- **router ospf**
- **stub cost**
- **virtuallink neighborid**
- **show ip ospf**
- **show ip ospfase**
- **show ip ospf cumulative**
- **show ip ospf database**
- **show ip ospf interface**
- **show ip ospf neighbor**
- **show ip ospf routing**
- **show ip ospf virtual-links**
- **show ip protocols**
- **debug ip ospf event**
- **debug ip ospf lsa**
- **debug ip ospf packet**
- **debug ip ospf spf**

15.4.2.2.1 default redistribute cost

Command: default redistribute cost <*cost*>
no default redistribute cost
Function: Sets the default cost for introducing exterior routes into OSPF; the "**no default redistribute cost**" command restores the default setting.
Parameter: < *cost*> is the route cost, ranging from 1 to 65535.
Default: The default introducing cost is 1.
Command Mode: OSPF protocol configuration mode
Usage Guide: When OSPF routing protocol introduce the routes discovered by the other routing protocols, those routes are regarded as the exterior autonomous system routing information. Introduction of exterior routing information requires some external parameter such as default cost and default tag for the routes. This command allow the user to set reasonable default cost for introducing exterior routes according to specific conditions,
Example: Set the default cost for OSPF to introduce exterior routes to 20.

Switch(Config-Router-Ospf)#default redistribute cost 20

15.4.2.2.2 default redistribute interval

Command: default redistribute interval <*time*>
no default redistribute interval
Function: Set the interval for introducing external routes; the "**no default redistribute interval**" command restores the default setting.
Parameter: <***time***> is the interval for introducing exterior routes in seconds; the valid range is 1 to 65535.

Default: The default interval in OSPF for introducing exterior routes is 1 second.

Command Mode: OSPF protocol configuration mode

Usage Guide: OSPF introduces exterior routing information regularly and advertise the information throughout the autonomous system. This command is used to modify the interval for introducing exterior routing information.

Example: Set the interval in OSPF for introducing exterior routes to 3 second.

Switch(Config-Router-Ospf)#default redistribute interval 3

15.4.2.2.3 default redistribute limit

Command: default redistribute limit <*routes*>

no default redistribute limit

Function: Set the maximum exterior routes allowed in one route introduction; the "**no default redistribute limit**" command restores the default setting.

Parameter: < *value*> is the maximum routes allowed in one route introduction, ranging from 1 to 65535.

Default: The default exterior route allowed to be introduced in OSPF is 100.

Command Mode: OSPF protocol configuration mode

Usage Guide: OSPF introduces exterior routing information regularly and advertise the information throughout the autonomous system. This command mandates the maximum exterior routes allowed in one route introduction.

Example: Set the maximum exterior routes allowed in one route introduction to 110.

Switch(Config-Router-Ospf)#default redistribute limit 110

15.4.2.2.4 default redistribute tag

Command: default redistribute tag <*tag*>

no default redistribute tag

Function: Set the tag value for introducing exterior routes; the "**no default redistribute tag**" command restores the default setting.

Parameter: < *tag*> is the tag value, ranging from 0 to 4294967295.

Default: The default tag value is 0.

Command Mode: OSPF protocol configuration mode

Usage Guide: When OSPF routing protocol introduce the routes discovered by the other routing protocols, those routes are regards as the exterior autonomous system routing information. Introduction of exterior routing information requires some external parameter such as default cost and default tag for the routes. This command provides the user with information about tag identifying protocols.

Example: Set the default tag value for OSPF to introduce exterior routes to 20000.

Switch(Config-Router-Ospf)#default redistribute tag 20000

15.4.2.2.5 default redistribute type

Command: default redistribute type { 1 | 2 }
no default redistribute type
Function: Set the default route type(s) for exterior routes introduction; the "**no default redistribute type**" command restores the default setting.
Parameter: 1 and **2** stand for type1 and type2 exterior routes, respectively.
Default: The system assumes to introduce Type2 exterior routes by default.

Command Mode: OSPF protocol configuration mode
Usage Guide: OSPF protocol divides exterior route information into 2 categories by cost selection method: type1 exterior route and type2 exterior route. The cost of type1 exterior route = advertised cost of exterior route + cost from a layer3 switch to the advertising layer3 switch (AS exterior layer3 switch). Cost of type2 exterior route = advertised cost of exterior route. If both type1 and type2 exterior routes present, type1 routes take precedence.
Example: Set the default exterior route type for OSPF to introduce to type1.
Switch(Config-Router-Ospf)#default redistribute type 1

15.4.2.2.6 ip ospf authentication

Command: ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>}
no ip ospf authentication
Function: Configure authentication method for the interface to accept OSPF packets; the "**no ip ospf authentication**" command cancels the authentication.
Parameter: simple stands for simple authentication; **md5** for MD5 encrypted authentication; ***<auth_key>*** for authentication key, which should be a string with no blank characters, up to 8 bytes in simple authentication and 16 bytes in MD5 authentication are allowed; ***<key_id>*** is the checksum word for MD5 authentication, range from 1 to 255.
Default: Authentication is not required by default for the interface to accept OSPF packets.

Command mode: Interface Mode
Usage Guide: The value of key will be written into the OSPF packets to ensure proper OSPF packet sending/receiving between the layer3 switch and neighbor layer3 switches. The partner end must have the same "*key*" parameters set.
Example: Configure MD5 authentication for OSPF interface vlan1 with an authentication password of "123abc".
Switch(Config-If-Vlan1)#ip ospf authentication md5 123abc 1

15.4.2.2.7 ip ospf cost

Command: ip ospf cost <*cost*>
no ip ospf cost

Function: Set the cost for running OSPF on the interface; the "**no ip ospf cost**" command restores the default setting.
Parameter: < *cost*> is the OSPF cost, ranging from 1 to 65535.
Default: The default cost for OSPF protocol is 1.

Command mode: Interface Mode
Example: Set the OSPF route cost of interface vlan1 to 3.
Switch(Config-If-Vlan1)#ip ospf cost 3

15.4.2.2.8 ip ospf dead-interval

Command: ip ospf dead-interval <*time* >
no ip ospf dead-interval
Function: Specify the interval before regarding a neighbor layer3 switch invalid; the "**no ip ospf dead-interval**" command restores the default setting.
Parameter: <***time***> is the timeout value for a neighbor layer3 switch to be considered invalid in seconds; the valid range is 1 to 65535.
Parameter: The default timeout value for a neighbor layer3 switch to be considered invalid is 40 seconds (usually 4 times of the hello-interval).

Command mode: Interface Mode
Usage Guide: If no HELLO packet is received from a neighbor layer3 switch within the **dead-interval** time, that switch is considered unreachable and invalid. This command allows the user to set default time of a neighbor layer3 switch to be considered invalid. The **dead-interval** value set will be written to the HELLO packet and send with it. For OSPF protocol to run properly,
the **dead-interval** parameter between the interface and a neighbor layer3 switch must be the same, and be at least four times of the **hello-interval** value.

Example: Set the OSPF route invalid timeout value of interface vlan1 to 80s.
Switch(Config-If-Vlan1)#ip ospf dead-interval 80

15.4.2.2.9 ospf enable area

Command: ip ospf enable area <*area_id*>
no ip ospf enable area
Function: Set an area for the interface; the "**no ip ospf enable area**" command cancels the setting.
Parameter: <*area_id*> is the area number where the interface resides, ranging from 0 to 4294967295.
Default: The interface has no area configured by default.
Command mode: Interface Mode
Usage Guide: To run OSPF protocol on an interface, an area must be specified for that

interface.

Example: Specify interface vlan1 to area 1.

Switch(Config-If-Vlan1)#ip ospf enable area 1

15.4.2.2.10 ip ospf hello-interval

Command: ip ospf hello-interval <*time*>

no ip ospf hello-interval

Function: Configure the interval for sending HELLO packets from the interface; the "**no ip ospf hello-interval**" command restores the default setting.

Parameter: <***time***> is the interval for sending HELLO packets in seconds, ranging from 1 to 255.

Default: The default HELLO-packet-sending interval is 10 seconds.

Command mode: Interface Mode

Usage Guide: The HELLO packet is a most common packet that is sent to neighbor layer3 switches regularly for discovering and maintaining the neighborhood and the election of DR and BDR. The **hello-interval** value set will be written to the HELLO packet and send with it. Smaller **hello-interval** enables faster discovery of network topology changes and incurs greater routing overhead. For OSPF protocol to run properly, the **hello-interval** parameter between the interface and the neighbor layer3 switch must be the same.

Example: Set the HELLO-packet-sending interval of interface vlan1 to 20 seconds.

Switch(Config-If-Vlan1)#ip ospf hello-interval 20

Related command: ip ospf dead-interval

15.4.2.2.11 ip ospf passive-interface

Command: ip ospf passive-interface

no ip ospf passive-interface

Function: Set an interface to receive OSPF packets only, the "no **ip ospf passive-interface"** command cancels the setting.

Default: The interface receives/sends OSPF packets by default.

Command mode: Interface Mode

Example: Set Ethernet interface vlan1 to receive OSPF packet only.

Switch(Config-If-Vlan1)#ip ospf passive-interface

15.4.2.2.12 ip ospf priority

Command: ip ospf priority <*priority*>

no ip ospf priority

Function: Set the priority of the interface in “designated layer3 switch” (DR) election; the “**no ip ospf priority**” command restores the default setting.

Parameter: **< *priority*>** is the priority value, ranging from 0 to 255.

Defaulted: The priority of the interface when electing designated layer3 switch is 1.

Command mode: Interface Mode

Usage Guide: When two layer3 switches in the same network segment want to be the “designated layer3 switch”(DR), the DR is decided by the priority value, the switch with higher priority becomes the DR; if priority values are equal, the switch with the larger router-id is selected. When a layer3 switch has a priority value of 0, it will not be elected to be either “designated layer3 switch” or “backup designated layer3 switch”.

Example: Configure the priority of the interface when electing designated layer3 switch (DR). Exclude interface vlan1 from the election, i.e., set the priority to 0.

Switch(Config-If-Vlan1)#ip ospf priority 0

15.4.2.2.13 ip ospf retransmit-interval

Command: ip ospf retransmit-interval <*time*>

no ip ospf retransmit-interval

Function: Set the interval for retransmission of link-state advertisement among neighbor layer3 switches; the “**no ip ospf retransmit**” command restores the default setting.

Parameter: <***time***> is the interval of link-state status advertisement retransmission to a neighbor layer3 switch in seconds, ranging from 1 to 65535.

Default: The default retransmission interval is 5 seconds.

Command mode: Interface Mode

Usage Guide: When a layer3 switch transfers link-state advertisement to its neighbor, it keeps advertising until an acknowledgement is received from the other end, if no acknowledge packet is received within the interval set, it will resend the link-state advertisement. The retransmission interval must be greater than the time for a packet to travel to a layer3 switch and return.

Example: Set the re-authentication time of LSA for interface vlan1 to 10 seconds.

Switch(Config-If-Vlan1)#ip ospf retransmit 10

15.4.2.2.14 ip ospf transmit-delay

Command: ip ospf tranmsit-delay <*time*>

no ip ospf transmit-delay

Function: Set the delay time before sending link-state advertisement (LSA); the "**no ip ospf transmit-delay**" command restores the default setting.

Parameter: <*time*> is the delay time for the link-state advertisement transmission in seconds, ranging from 1 to 65535.

Default: The default LSA sending interval is 1 second.

Command mode: Interface Mode

Usage Guide: LSA aging occurs on the local layer3 switch but not during network transmission, therefore, adding a delay of **transmit-delay** allows the LSA to be sent before it is aged.

Example: Set the delay time for interface vlan1 to send LSA to 2 seconds.

Switch(Config-If-Vlan1)#ip ospf transmit-delay 2

15.4.2.2.15 network

Command: network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]

no network <*network*> <*mask*> area <*area_id*>

Function: Specify the area of each network in the layer3 switch; the "**no network <*network*> <*mask*> area <*area_id*>"** command deletes the setting.

Parameter: <*network*> and **<*mask*>** are the network IP address and mask in dotted decimal format; **<*area_id*>** is the area number from 0 to 4294967295; **advertise | notadvertise** specifies whether or not broadcast the summary route information within the network.

Default: The system has no default area configure; if configured, it assumes to broadcast summary information by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: Once a part of a network joins an area, all interior routes of that network will no longer be broadcasted to the other areas independently, but the summary information for that whole network. The introduction of network scope and scope limit can reduce the routing information traffic between areas.

Example: Specify network scope 10.1.1.0, 255.255.255.0 to join area 1.

Switch(Config-Router-Ospf)#network 10.1.1.0 255.255.255.0 area 1

15.4.2.2.16 preference

Command: preference [ase] <*preference* >

no preference [ase]

Function: Configure the priority of OSPF among all the routing protocols, and the priority

for AS exterior routes introduced; the "**no preference [ase]**" command restores the default setting.

Parameter: ase means the priority is used when introducing exterior routes outside the AS; ***<preference >*** is the priority value ranging from 1 to 255.

Default: The default priority of OSPF protocol is 110; the default priority to introduce exterior route is 150.

Command Mode: OSPF protocol configuration mode

Usage Guide: As a layer3 switch may have several dynamic routing protocol running, there arises the issue of information sharing and selection among routing protocols. For this reason, each routing protocol has a default priority,. When the same route is discovered by different protocols, the one with the higher priority overrules. Priority changes will be applied on newly constructed routes. Due to the nature of OSPF, the OSPF priority should not be set too low.

Example: Set in OSPF the default priority to introduce ASE route to 20.

Switch(Config- Router-Ospf)#preference ase 20

15.4.2.2.17 redistribute ospfase

Command: redistribute ospfase { bgp |connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>]

no redistribute ospfase { bgp |connected | static | rip}

Function: Introduce BGP routes, direct routes, static routes and RIP routes as external routing information; the "no redistribute ospfase { bgp | connected | static | rip }" command cancels the introduction of external routing information.

Parameter: bgp stands for introduce BGP routes as the exterior route information source; **connected** for direct routes; **static** for static routes; **rip** for routes discovered by RIP; **type** specifies the type of exterior routes, **1** and **2** represent type1 exterior routes and type2 exterior routes, respectively; **tag** specifies the tag of the routes, ***<tag>*** is the tag value for the routes, ranging from 0 to 4,294,967,295; **metric** specifies the weight of the route; ***<cost_value>*** for weight value, ranging from 1 to 16,777,215.

Default: Exterior routes are not introduced in OSPF by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: Routing information can be shared among all dynamic routing protocols in layer3 switches. Due to the nature of OSPF, the routes discovered by the other routing protocols are regards as the exterior autonomous system routing information.

Example: introduce RIP routes as type1 exterior routes in OSPF, with a tag value of 3 and an introducing cost of 20.

Switch(Config-Router-Ospf)#redistribute ospfase rip type 1 tag 3 metric 20

15.4.2.2.18 router id

Command: router id <*router_id*>

no router id

Function: Configure the ID number for the layer3 switch running OSPF; the "**no router id**" command cancels the ID number.

Parameter: <*router_id*> is the ID number for the layer3 switch in dotted decimal format.

Default: No layer3 switch ID number is configured by default, an address from the IP addresses of all the interfaces is selected to be the layer3 switch ID number.

Command mode: Global Mode

Usage Guide: OSPF use the layer3 switch ID number as a unique identity for the layer3 switch in the autonomous system, usually the address of an interface running OSPF is selected to be the layer3 switch ID number ES4626/ES4650 layer3 switch used the first UP layer3 interface in the switch as the router id by default. If no IP address is configured in all interfaces of the layer3 switch, this command must be used to specify the layer3 switch ID number, otherwise OSPF would not work. Changes to a layer3 switch ID number will apply only after the restart of OSPF.

Example: Configure the ID of the layer3 switch to 10.1.120.1.

Switch(Config)#router id 10.1.120.1

15.4.2.2.19 router ospf

Command: router ospf

no router ospf

Function: Enable OSPF protocol and enter OSPF mode after enabling; the "**no router ospf**" command disables OSPF protocol.

Default: OSPF is disabled by default.

Command mode: Global Mode

Usage Guide: Use this command to enable or disable OSPF protocol. Configurations to OSPF will only take effect when OSPF is enabled.

Example: Enable OSPF on the switch.

Switch(Config)#router ospf

15.4.2.2.20 stub cost

Command: stub cost <*cost*> area <*area_id* >

no stub area <*area_id* >

Function: Set an area to STUB area; the "**no stub area <area_id >"** command cancels the setting.

Parameter: <*cost*> is the default route cost for the STUB area, ranging from 1 to 65535; **<*area_id* >** is the area number of the STUM area, ranging from 1 to 4,294,967,295.

Default: No STUB area is configured by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: An area can be configured to a STUB area if the area has only one egress point (connect to one layer3 switch only), or need not select egress point for each exterior destination. Type4 LSA (ASBR summary LSA) and type5 LSA (AS exterior LSA) are not allowed to flood into/through STUB areas, this saves the resource for processing exterior routing information for layer3 switches inside the area.

Example: Set area 1 to be a STUB area with a default routing cost of 60.

Switch(Config-Router-Ospf)#stub cost 60 area 1

15.4.2.2.21 virtuallink neighborid

Command: virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit<*time*>] [transitdelay <*time*>]
no virtuallink neighborid <*router_id*> transitarea <*area_id*>

Function: Create and configure virtual link; the "**no virtuallink neighborid <*router_id*> transitarea <*area_id*>**" command deletes a virtual link.

Parameter: is the ID for the virtual link neighbor in dotted decimal format; is the area number for transit area, ranging from 0 to 42,949,67,295; the rest four parameters are optional intervals that has the same meaning as those in OSPF interface mode.

Default: No virtual link is configured by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: The introduction of virtual link is to fulfill or enhance the connectivity of the backbone area (area 0). As the backbone area must keep connected logically, if no in-area route exists between two nodes within the backbone area, a virtual link must be established between the two nodes across a transit area. Virtual link is identified by the ID of the partner layer3 switch. The non-backbone area providing interior route for both ends of the virtual link is referred to a "transit area", the area number must be specified on configuration.

A virtual link is activated when the route across the transit area is calculated, and practically forms a point-to-point connection between the two ends. In this connection, interface parameters (such as HELLO interval) can be configured just as on a physical interface.

Example: Configure a virtual link to 11.1.1.1 via transit area 2.

Switch(Config-Router-Ospf)#virtuallink neighborid 11.1.1.1 transitarea 2

15.4.2.2.22 show ip ospf

Command: show ip ospf

Function: Display major OSPF information.

Default: Not displayed.

Command mode: Admin Mode

Example:

```
Switch#show ip ospf
my router ID is 11.11.4.1
preference=10     ase perference=150
export metric=1
export tag=-2147483648
area ID   0
    interface count: 1
    80times spf has been run for this area
    net range:
LSRefreshTime is1800
area ID   1
    interface count: 1
    41times spf has been run for this area
    net range:
netid11.11.3.255     netaddress11.11.0.0     netmask255.255.252.0
LSRefreshTime is1800
```

Displayed information	Explanation
my router ID	The ID of the current layer3 switch.
preference	Routing protocol priority.
ase perference	Exterior routes priority for introduction.
export metric	The metrics for output from the port
export tag	The route tag for output from the port.
area ID interface count imes spf has been run for this area net range	OSPF area number: including statistics for interface number in the area, SPF algorithm calculation time and network scope.

15.4.2.2.23 show ip ospf ase

Command: show ip ospf ase

Function: Display exterior OSPF routing information.

Default: Not displayed.

Command mode: Admin Mode

Example:

```
Switch#show ip ospf ase
Destination     AdvRouter    NextHop    Age    SeqNumber      Type    Cost
10.1.1.125      11.11.1.2    11.1.1.2   3      300            2       20
```

Displayed information	Explanation
Destination	Target network segment or address
AdvRouter	Route election
NextHop	Next hop address
Age	Aging time.
SeqNumber	Sequence number.
Type	Exterior routes type for introduction.
Cost	Cost for introducing exterior routes

15.4.2.2.24 show ip ospf cumulative

Command: show ip ospf cumulative

Function: Display OSPF statistics.

Default: Not displayed.

Command mode: Admin Mode

Example:

Switch#show ip ospf cumulative

IO cumulative

type in out

HELLO 1048 253

DD 338 337

LS Req 62 219

LS Update 753 295

LS Ack 495 308

ASE count 0 checksum 0

original LSA 340 LS_RTR 179 LS_NET 1 LS_SUM_NET 160 LS_SUM_ASB 0 LS_ASE 0

received LSA 325

Areaid 0

nbr count 1 interface count 1

spf times 120

DB entry count 6

LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3

Areaid 1

nbr count 2 interface count 1

spf times 52

DB entry count 6

LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3

AS internal route 4 AS external route 0

Displayed information	Explanation
IO cumulative	Statistics for OSPF packets in/out.
type	Packet type: including HELLO packet, DD packet, LS request, update and acknowledging packet, etc.
In	Packet in statistics.
Out	Packet out statistics.
Areaid	OSPF statistics from a specific OSPF area.

15.4.2.2.25 show ip ospf database

Command: show ip ospf database [{asb-summary| external | network | router | summary}]

Function: Display OSPF link-state database information.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: OSPF link-state database information can be checked by the output of this command.

Example:

Switch#show ip ospf database

OSPF router ID: 11.11.4.1 AS: No

Area 1>>>>>>>> Area ID: 0

Router LSAs

LS ID (Router ID)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Router LSA

11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Network LSAs

LS ID (DR's IP)	ADV rtr	Age	Sequence	Cost	Checksum

11.11.4.2	11.11.4.2	1	2147483662	1	35126

Summary Network LSAs

LS ID (Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.1.0	11.11.4.1	0	2147483656	1	6777215
11.11.2.255	11.11.4.1	0	2147483649	1	6777215
11.11.3.255	11.11.4.1	0	2147483680	1	6777215

ASBR Summary LSAs

LS ID (ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum

Area 2>>>>>>>> Area ID: 1

Router LSAs

LS ID (Router ID)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875
Router LSA					
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Network LSAs

LS ID (DR's IP)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.1.1	11.11.4.1	0	2147483649	1	6777215
11.11.1.3	14.14.14.1	15	2147483705	1	53384

Summary Network LSAs

LS ID (Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.255	11.11.4.1	0	2147483677	1	6777215

ASBR Summary LSAs

LS ID (ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum

AS External LSAs

LS ID Route type ADV rtr Age Sequence Cost Checksu Forw addr RouteTag (Ext Net's IP)

Displayed information	Explanation
OSPF router ID	The ID of the layer3 switch.
Area 1>>>>>>>> Area ID: 0	Represent the LSA database information from area 1 to area 0.
Router LSAs	Route LSA
Network LSAs	Network LSA
Summary Network LSAs	Summary network LSA
ASBR Summary LSAs	Autonomous system exterior LSA

15.4.2.2.26 show ip ospf interface

Command: show ip ospf interface *<interface>*

Function: Display OSPF interface information.

Parameter: *<interface>* stands for the interface name.

Default: Not displayed.

Command mode: Admin Mode

Example:

Switch#show ip ospf interface vlan 1
IP address: 11.11.4.1 Mask: 255.255.255.0 Area: 0
Net type: BROADCAST cost: 1
State: IBACKUP Type: BDR
Priority: 1 Transit Delay: 1
DR: 11.11.4.2 BDR: 11.11.4.1
Authentication key:
Timer: Hello: 10 Poll: 0 Dead: 40 Retrans: 5
Number of Neigbors: 1 Nubmer of Adjacencies: 1
Adjacencies:
1: 11.11.4.2

Displayed information	Explanation
IP address	Interface IP address
Mask	Interface mask.
Area	The area of the interface
Net type	Network type, such as broadcast, p2mp, etc.
cost	Cost value.
State	Status

Type	layer3 switch type, such as designated layer3 switch.
Priority	Configure the priority in electing designated layer3 switch.
Transit Delay	The delay value for interface to transfer LAS.
DR	The designated layer3 switch.
BDR	Backup designated layer3 switch.
Authentication key	OSPF packet authentication key.
Timer: Hello、Poll、Dead、Retrans	OSPF protocol timer: including time set for HELLO packet, poll interval packet, route invalid, route retransmission, etc.
Number of Neigbors	The number of neighboring layer3 switches.
Nubmer of Adjacencies	The number of neighboring route interfaces.
Adjacencies	Neighboring interface IP address

15.4.2.2.27 show ip ospf neighbor

Command: show ip ospf neighbor

Function: Display OSPF neighbor node information.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: OSPF neighbor information can be checked by the output of this command.

Example:

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1       area id 0
   router id 12.1.1.2        router ip addr 12.1.1.2
   state NFULL       priority 1
   DR 12.1.1.2        BDR 12.1.1.1
   last hello 59006       last exch 49717
interface ip 30.1.1.1       area id 0
interface ip 50.1.1.1       area id 0
   router id 50.1.1.2        router ip addr 50.1.1.2
   state NFULL       priority 0
   DR 50.1.1.1        BDR 0.0.0.0
   last hello 59010       last exch 49614
```

interface ip 51.1.1.1 area id 0
interface ip 52.1.1.1 area id 0
interface ip 100.1.1.1 area id 0
interface ip 110.1.1.1 area id 0
interface ip 150.1.1.1 area id 0
router id 12.2.0.0 router ip addr 150.1.1.2
state NFULL priority 0
DR 150.1.1.1 BDR 0.0.0.0
last hello 59011 last exch 49607

Displayed information	Explanation
interface ip	The IP address of an interface in the current layer3 switch.
area id	The id of the area for the interface
router id	The ID of the neighbor layer3 switch.
router ip addr	The IP address of the interface in the neighbor layer3 switch.
state	Link-state status
priority	Priority.
DR	ID of the designated layer3 switch.
BDR	ID of the backup designated layer3 switch.
last hello	The last HELLO packet.
last exch	The last packet exchanged.

15.4.2.2.28 show ip ospf routing

Command: show ip ospf routing

Function: Display OSPF route table information.

Default: Not displayed.

Command mode: Admin Mode

Example:

Switch#show ip ospf routing

AS internal routes:

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
60.2.127.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.1.132.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.4.67.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.3.72.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.2.77.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2

AS external routes:

Destination Cost Dest Type Next Hop ADV rtr

Displayed information	Explanation
AS internal routes	Autonomous system interior route.
AS external routes	Autonomous system exterior route.
Destination	Destination network segment
Area	Area number.
Cost	Cost value.
Dest Type	Route Type
Next Hop	Next hop
ADV rtr	Advertise the interface address of the layer3 switch.

15.4.2.2.29 show ip ospf virtual-links

Command: show ip ospf virtual-links

Function: Display OSPF virtual link information.

Default: Not displayed.

Command mode: Admin Mode

Example:

Switch#show ip ospf virtual-links

no virtual-link

15.4.2.2.30 show ip protocols

Command: show ip protocols

Function: Display the information of the routing protocols running in the switch.

Command mode: Admin Mode

Usage Guide: The user can decide whether the routing protocols configured are correct and perform routing troubleshooting according to the output of this command.

Example:

Switch#sh ip protocols
OSPF is running.
my router ID is 100.1.1.1
preference=10 ase perference=150
export metric=1
export tag=-2147483648
area ID 1

interface count: 2
7times spf has been run for this area
net range:
LSRefreshTime is1800
RIP information
rip is shutting down

Displayed information	Explanation
OSPF is running	The running routing protocol is OSPF protocol.
My router ID	The ID number of the layer3 switch running.
Preference	OSPF routing priority.
Ase perference	Autonomous system exterior routes priority
Export metric	Metrics for exporting OSPF routes.
Export tag	Tag value for exporting OSPF routes.
Area ID	The ID of the OSPF area that the current layer3 switch resides.
Interface count	Number of interface running OSPF routing protocol
N times spf has been run for this area	The layer3 switch performs minimum tree spanning calculation.
Net range	The network scope for running OSPF protocol.
LSRefreshTime	Link-state advertisement (LSA) update interval of OSPF protocol.

15.4.2.2.31 debug ip ospf event

Command: debug ip ospf event
no debug ip ospf event

Function: Enable the OSPF debug function for all events: the "**no debug ip ospf event**" command disables the debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

15.4.2.2.32 debug ip ospf lsa

Command: debug ip ospf lsa
no debug ip ospf lsa

Function: Enable the link-state status advertisement debug function: the "**no debug ip ospf lsa**" command disables the debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

15.4.2.2.33 debug ip ospf packet

Command: debug ip ospf packet

no debug ip ospf packet

Function: Enable the OSPF packet debug function; the "**no debug ip ospf packet**" command disables this debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ip ospf packet

packet length: 44

02: 40: 54:

receive ACK from 11.11.1.3

02: 40: 56:

receive a packet from 11.11.1.2

packet length: 44

02: 40: 56:

receive ACK from 11.11.1.2

02: 40: 58:

receive a packet from 11.11.4.2

packet length: 48

02: 40: 58:

receive a HELLO packet from 11.11.4.2 via Broadcast interface 11.11.4.1

02: 40: 58:

15.4.2.2.34 debug ip ospf spf

Command: debug ip ospf spf

no debug ip ospf spf

Function: Enable the OSPF debug function for shortest path algorithm; the "**no debug ip ospf spf**" command disables this debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

15.4.3 Typical OSPF Scenario

Scenario 1: OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five ES4626/ES4650 layer3 switches for example, where layer3 switch Switch1 and Switch5 make up OSPF area 0, layer3 switch Switch2 and Switch3 form OSPF area 1 (assume vlan1 interface of layer3 switch Switch1 belongs to area 0), layer3 switch Switch4 forms OSPF area2 (assume vlan2 interface of layer3 Switch5 belongs to area 0). Swtich1 and Switch5 are backbone layer3 switches, Swtich2 and Switch4 are area edge layer3 switches, and Switch3 is the in-area layer3 switch.

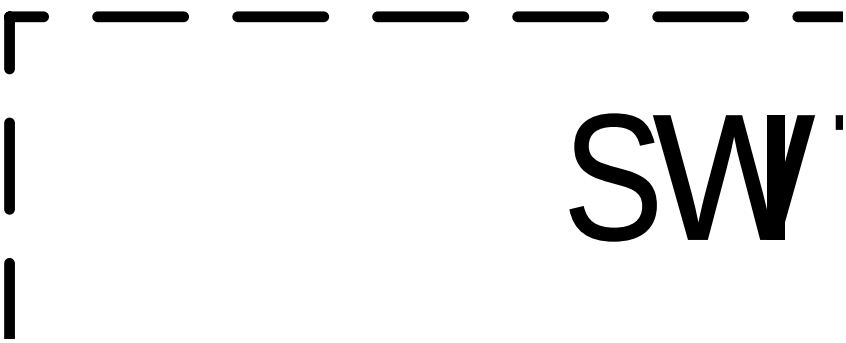


Fig 15-3 Network topology of OSPF autonomous system.

The configuration for layer3 switch Switch1 and Switch5 is shown below:

Layer3 switch Switch1:

!Configuration of the IP address for interface vlan1

Switch1#config

Switch1(Config)# interface vlan 1

Switch1(Config-if-vlan1)# ip address 10.1.1.1 255.255.255.0

Switch1(Config-if-vlan1)#no shut-down

Switch1(Config-if-vlan1)#exit

! Configuration of the IP address for interface vlan2

Switch1(Config)# interface vlan 2

Switch1(Config-if-vlan2)# ip address 100.1.1.1 255.255.255.0

Switch1 (Config-if-vlan2)#exit

! Enable OSPF protocol, configure the area number for interface vlan1 and vlan2.

Switch1(Config)#router ospf

Switch1(Config-router-ospf)#exit

Switch1(Config)#interface vlan 1

Switch1 (Config-if-vlan1)#ip ospf enable area 0

Switch1 (Config-if-vlan1)#exit

```
Switch1(Config)#interface vlan2
Switch1 (Config-if-vlan2)#ip ospf enable area 0
Switch1 (Config-if-vlan2)#exit
Switch1(Config)#exit
Switch1#
Layer3 switch Switch2:
!Configure the IP address for interface vlan1 and vlan2.
Switch2#config
Switch2(Config)# interface vlan 1
Switch2(Config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
Switch2(Config-if-vlan1)#no shut-down
Switch2(Config-if-vlan1)#exit
Switch2(Config)# interface vlan 3
Switch2(Config-if-vlan3)# ip address 20.1.1.1 255.255.255.0
Switch2(Config-if-vlan3)#no shut-down
Switch2(Config-if-vlan3)#exit
！Enable OSPF protocol, configure the OSPF area interfaces vlan1 and vlan3 in.
Switch2(Config)#router ospf
Switch2(Config-router-ospf)#exit
Switch2(Config)#interface vlan 1
Switch2(Config-if-vlan1)#ip ospf enable area 0
Switch2(Config-if-vlan1)#exit
Switch2(Config)#interface vlan 3
Switch2(Config-if-vlan3)#ip ospf enable area 1
Switch2(Config-if-vlan3)#exit
Switch2(Config)#exit
Switch2#
Layer3 switch Switch3:
!Configuration of the IP address for interface vlan3
Switch3#config
Switch3(Config)# interface vlan 3
Switch3(Config-if-vlan1)# ip address 20.1.1.2 255.255.255.0
Switch3(Config-if-vlan3)#no shut-down
Switch3(Config-if-vlan3)#exit
！Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.
Switch3(Config)#router ospf
Switch3(Config-router-ospf)#exit
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip ospf enable area 1
```

```
Switch3(Config-if-vlan3)#exit
Switch3(Config)#exit
Switch3#
Layer3 switch Switch4:
!Configuration of the IP address for interface vlan3
Switch4#config
Switch4(Config)# interface vlan 3
Switch4(Config-if-vlan3)# ip address30.1.1.2 255.255.255.0
Switch4(Config-if-vlan3)#no shut-down
Switch4(Config-if-vlan3)#exit
！ Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.
Switch4(Config)#router ospf
Switch4(Config-router-ospf)#exit
Switch4(Config)#interface vlan 3
Switch4(Config-if-vlan3)#ip ospf enable area 0
Switch4(Config-if-vlan3)#exit
Switch4(Config)#exit
Switch4#
Layer3 switch Switch5:
!Configuration of the IP address for interface vlan2
Switch5#config
Switch5(Config)# interface vlan 2
Switch5(Config-if-vlan2)# ip address 30.1.1.1 255.255.255.0
Switch5(Config-if-vlan2)#no shut-down
Switch5(Config-if-vlan2)#exit
! Configuration of the IP address for interface vlan3
Switch5(Config)# interface vlan 3
Switch5(Config-if-vlan3)# ip address 100.1.1.2 255.255.255.0
Switch5(Config-if-vlan3)#no shut-down
Switch5(Config-if-vlan3)#exit
 ！ Enable OSPF protocol, configure the number of the area in which interface vlan2
  and vlan3 reside in.
Switch5(Config)#router ospf
Switch5(Config-router-ospf)#exit
Switch5(Config)#interface vlan 2
Switch5(Config-if-vlan2)#ip ospf enable area 0
Switch5(Config-if-vlan2)#exit
Switch5(Config)#interface vlan 3
Switch5(Config-if-vlan3)#ip ospf enable area 0
```

Switch5(Config-if-vlan3)#exit

Switch5(Config)#exit

Switch5#

Scenario 2: Typical OSPF protocol complex topology.

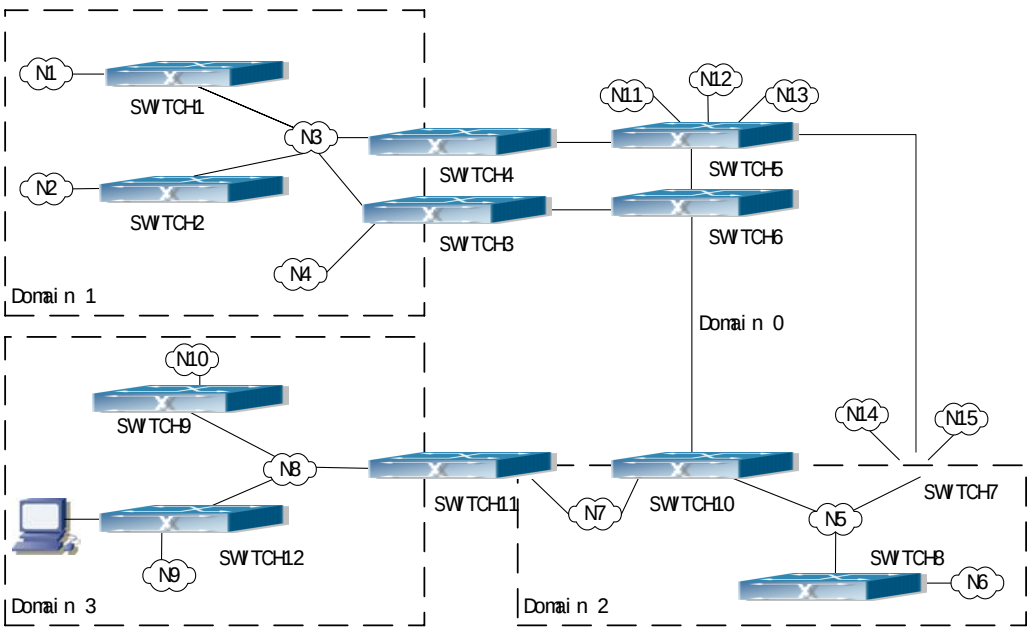


Fig 15-4 Typical complex OSPF autonomous system.

The figure is a typical complex OSPF autonomous system network topology. Area1 include network N1-N4 and layer3 switch Switch1-Switch4, area2 include network N5-N7 and layer3 switch Switch7, Switch8, Switch10 and Switch11, area3 include N8-N10, host H1 and layer3 switch Switch9, Switch11 and Switch12, and network N8-N10 share a same summary route with host H1(i.e. define area3 and a STUB area). Layer3 switch Switch1, Switch2, Switch5, Switch6, Switch8, Switch9, Switch12 are in-area layer3 switches, Switch3, Switch4, Switch7, Switch10 and Switch11 are edge layer3 switches of the area, Switch5 and Switch7 are edge layer3 switches of the autonomous system.

To area1, layer3 switches Switch1 and Switch2 are both in-area switches, area edge switches Switch3 and Switch4 are responsible for reporting distance cost to all destination outside the area, while they are also responsible for reporting the position of the AS edge layer3 switches Switch5 and Switch7, AS exterior link-state advertisement from Switch5 and Switch7 are flooded throughout the whole autonomous system. When ASE LSA

floods in area 1, those LSA are included in the area 1 database to get the routes to network N11 and N15.

In addition, layer3 switch Switch3 and Switch4 must summary the topology of area 1 to the backbone area (area 0, all non-0 areas must be connected via area 0, direct connections are not allowed), and advertise the networks in area 1 (N1-N4) and the costs from Switch3 and Switch4 to those networks. As the backbone area is required to keep connected, there must be a virtual link between backbone layer3 switch Switch10 and Switch11. The area edge layer3 switches exchange summary information via the backbone layer3 switch, each area edge layer3 switch listens to the summary information from the other edge layer3 switches.

Virtual link can not only maintain the connectivity of the backbone area, but also strengthen the backbone area. For example, if the connection between backbone layer3 switch Switch8 and Switch10 is cut down, the backbone area will become discontinued. The backbone area can become more robust by establishing a virtual link between backbone layer3 switches Switch7 and Switch10. In addition, the virtual link between Switch7 and Switch10 provide a short path from area 3 to layer3 switch Switch7.

Take area 1 as an example. Assume the IP address of layer3 switch Switch1 is 10.1.1.1, IP address of layer3 switch Switch2 interface VLAN2 is 10.1.1.2, IP address of layer3 switch Switch3 interface VLAN2 is 10.1.1.3, IP address of layer3 switch Switch4 interface VLAN2 is 10.1.1.4. Switch1 is connecting to network N1 through Ethernet interface VLAN1 (IP address 20.1.1.1); Switch2 is connecting to network N2 through Ethernet interface VLAN1 (IP address 20.1.2.1); Switch3 is connecting to network N4 through Ethernet interface VLAN3 (IP address 20.1.3.1). All the three addresses belong to area 1. Switch3 is connecting to layer3 switch Switch6 through Ethernet interface VLAN1 (IP address 10.1.5.1); Switch4 is connecting to layer3 switch Switch5 through Ethernet interface VLAN1 (IP address 10.1.6.1); both two addresses belong to area 1. Simple authentication is implemented among layer3 switches in area1, edge layer3 switches of area 1 authenticate with the area 0 backbone layer3 switches by MD5 authentication.

The followings are just configurations for all layer3 switches in area 1, configurations for layer3 switches of the other areas are omitted. The following are the configurations of Switch1 Switch2.Switch3 and Switch4: :

1)Switch1:

```
!Configuration of the IP address for interface vlan2
Switch1#config
Switch1(Config)# interface vlan 2
Switch1(Config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0
Switch1(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch1(Config)#router ospf
Switch1(Config-router-ospf)#exit
Switch1(Config)#interface vlan 2
Switch1(Config-If-Vlan2)#ip ospf enable area 1

!Configure simple key authentication.
Switch1(Config-If-Vlan2)#ip ospf authentication simple key
```

```
Switch1(Config-If-Vlan2)exit
!Configuration of the IP address and area number for interface vlan1
Switch1(Config)# interface vlan 1
Switch1(Config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
Switch1(Config-If-Vlan1)#ip ospf enable area 1
Switch1(Config-If-Vlan1)#exit
2)Switch2:
!Configuration of the IP address for interface vlan2
Switch2#config
Switch2(Config)# interface vlan 2
Switch2(Config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0
Switch2(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch2(Config)#router ospf
Switch2(Config-router-ospf)#exit
Switch2(Config)#interface vlan 2
Switch2(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch2(Config-If-Vlan2)#ip ospf authentication simple key
Switch2(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan1
Switch2(Config)# interface vlan 1
Switch2(Config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
Switch2(Config-If-Vlan1)#ip ospf enable area 1
Switch2(Config-If-Vlan1)#exit
Switch2(Config)#exit
Switch2#
3)Switch3:
!Configuration of the IP address for interface vlan2
Switch3#config
Switch3(Config)# interface vlan 2
Switch3(Config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
Switch3(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch3(Config)#router ospf
Switch3(Config-router-ospf)#exit
Switch3(Config)#interface vlan 2
Switch3(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch3(Config-If-Vlan2)#ip ospf authentication simple key
```

```
Switch3(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan3
Switch3(Config)# interface vlan 3
Switch3(Config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
Switch3(Config-If-Vlan3)#ip ospf enable area 1
Switch3(Config-If-Vlan3)#exit
!Configuration of the IP address and area number for interface vlan1
Switch3(Config)# interface vlan 1
Switch3(Config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
Switch3(Config-If-Vlan1)#ip ospf enable area 0
!Configure MD5 key authentication.
Switch3 (Config-If-Vlan1)#ip ospf authentication md5 key
Switch3 (Config-If-Vlan1)#exit
Switch3(Config)#exit
Switch3#
```

4)Switch4:

```
!Configuration of the IP address for interface vlan2
Switch4#config
Switch4(Config)# interface vlan 2
Switch4(Config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
Switch4(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch4(Config)#router ospf
Switch4(Config-router-ospf)#exit
Switch4(Config)#interface vlan 2
Switch4(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch4(Config-If-Vlan2)#ip ospf authentication simple key
Switch4(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan1
Switch4(Config)# interface vlan 1
Switch4(Config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
Switch4(Config-If-Vlan1)#ip ospf enable area 0
!Configure MD5 key authentication.
Switch4(Config-If-Vlan1)#ip ospf authentication md5 key
Switch4(Config-If-Vlan1)exit
Switch4(Config)#exit
Switch4#
```

15.4.4 OSPF Troubleshooting Help

1. Monitor and Debugging Commands
2. OSPF Troubleshooting Help

15.4.4.1 Monitor and Debugging Commands

Command	Explanation
Admin Mode	
Show interface status	Displays interface information to verify the interface and datalink layer protocols are up.
Show ip ospf	Displays the current running status and configuration information for OSPF. The user can decide whether the configurations are correct or not and perform OSPF troubleshooting according to the output of this command.
Show ip route	Displays route table information, OSPF routing information can be checked.
Show ip ospf ase	Displays exterior OSPF routing information.
Show ip ospf cumulative	Displays OSPF statistics.
Show ip ospf database	Displays OSPF link-state database information.
Show ip ospf interface	Displays OSPF information for the specified interface.
Show ip ospf neighbor	Displays OSPF neighbor information.
Show ip ospf routing	Displays OSPF route table information.
Show ip ospf virtual-links	Displays OSPF virtual link information.
Show ip protocols	Displays information for running routing protocols.
[no] debug ip ospf event	Displays all event information for OSPF debug; the "**no debug ip ospf event**" command disables this debug function.
[no] debug ip ospf lsa	Displays information for link-state advertisements; the "**no debug ip ospf lsa**" command disables this debug function.
[no] debug ip ospf packet	Displays information for OSPF packets; the "**no debug ip ospf packet**" command disables this debug function.
[no] debug ip ospf spf	Displays SPF information for debug; the "**no debug ip ospf spf**" command disables this debug function.

（1）show ip ospf

Example:

```
Switch#show ip ospf
my router ID is 11.11.4.1
preference=10     ase perference=150
export metric=1
export tag=-2147483648
area ID    0
    interface count: 1
    80times spf has been run for this area
    net range:
LSRefreshTime is1800
area ID    1
    interface count: 1
    41times spf has been run for this area
    net range:
netid11.11.3.255     netaddress11.11.0.0     netmask255.255.252.0
LSRefreshTime is1800
```

Displayed information	Explanation
my router ID	The ID of the current layer3 switch.
preference	Routing protocol priority.
ase perference	Exterior routes priority for introduction.
export metric	The hops for output from the port
export tag	The route tag for output from the port.
area ID interface count imes spf has been run for this area net range	OSPF area number: including statistics for interface number in the area, SPF algorithm calculation time and network scope.

（2）show ip route

The “show ip route” command can be used to display the information about OSPF routes in the route table: destination IP addresses, network masks, next hop IP addresses, and forwarding interfaces, etc.

For example, displayed information can be:

```
Switch#show ip route
Total route items is 4018, the matched route items is 4018
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
           A - OSPF ASE, B - BGP derived, D - DVMRP derived

    Destination        Mask              Nexthop          Interface        Preference
C   4.1.140.0          255.255.255.0     0.0.0.0          Vlan2139         0
```

A	5.1.1.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.2.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.3.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.4.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.5.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.6.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.7.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.8.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.9.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.10.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.11.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.12.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.13.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.14.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.15.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.16.0	255.255.255.0	12.1.1.2	Vlan12	150
O	5.1.17.0	255.255.255.0	12.1.1.2	Vlan12	110

---More---

Where, O stands for OSPF route, i.e., the OSPF route with the destination network address of 5.1.17.0, network mask of 255.255.255.0, the next hop address of 12.1.1.2 and the forwarding interface of Ethernet vlan12. The priority value of this route is 110.

（3）show ip ospf ase

The “show ip ospf ase” command can be used to display information about OSPF autonomous system exterior routes.

For example, displayed information can be:

Switch#show ip ospf ase

Destination	AdvRouter	NextHop	Age	SeqNumber	Type	Cost
10.1.1.125	11.11.1.2	11.1.1.2	3	300	2	20

Displayed information	Explanation
Destination	Target network segment or address.
AdvRouter	Route election
NextHop	Next hop address
Age	Aging time.
SeqNumber	Sequence number.
Type	Exterior routes type for introduction.
Cost	Cost for introducing exterior routes

（4）show ip ospf cumulative

The “show ip ospf cumulative” command can be used to display statistics about the OSPF protocol.

For example, displayed information can be:

Switch#show ip ospf cumulative
IO cumulative
type in out
HELLO 1048 253
DD 338 337
LS Req 62 219
LS Update 753 295
LS Ack 495 308
ASE count 0 checksum 0
original LSA 340 LS_RTR 179 LS_NET 1 LS_SUM_NET 160 LS_SUM_ASB 0 LS_ASE 0
received LSA 325
Areaid 0
nbr count 1 interface count 1
spf times 120
DB entry count 6
LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3
Areaid 1
nbr count 2 interface count 1
spf times 52
DB entry count 6
LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3
AS internal route 4 AS external route 0

Displayed information	Explanation
IO cumulative	Statistics for OSPF packets in/out.
type	Packet type: including HELLO packet, DD packet, LS request, update and acknowledging packet, etc.
In	Packet in statistics.
Out	Packet out statistics.
Areaid	OSPF statistics fro a specific OSPF area.

（5）show ip ospf database

The “show ip ospf database” command can be used to display information about the link-state database for OSPF protocol.

For example, displayed information can be:

Switch#show ip ospf database
OSPF router ID: 11.11.4.1 AS: No
Area 1>>>>>>>> Area ID: 0
Router LSAs
LS ID ADV rtr Age Sequence Cost Checksum

(Router ID)

11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Router LSA

11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(DR's IP)					
11.11.4.2	11.11.4.2	1	2147483662	1	35126

Summary Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Net's IP)					
11.11.1.0	11.11.4.1	0	2147483656	1	6777215
11.11.2.255	11.11.4.1	0	2147483649	1	6777215
11.11.3.255	11.11.4.1	0	2147483680	1	6777215

ASBR Summary LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(ASBR's Rtr ID)					

Area 2>>>>>>>> Area ID: 1

Router LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Router ID)					
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Router LSA

11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum

(DR's IP)

11.11.1.1 11.11.4.1 0 2147483649 1 6777215

11.11.1.3 14.14.14.1 15 2147483705 1 53384

Summary Network LSAs

LS ID ADV rtr Age Sequence Cost Checksum

(Net's IP)

11.11.4.255 11.11.4.1 0 2147483677 1 6777215

ASBR Summary LSAs

LS ID ADV rtr Age Sequence Cost Checksum

(ASBR's Rtr ID)

AS External LSAs

LS ID Route type ADV rtr Age Sequence Cost Checksu Forw addr RouteTag

(Ext Net's IP)

Displayed information	Explanation
OSPF router ID	The ID of the layer3 switch.
Area 1>>>>>>>> Area ID: 0	Represent the LSA database information from area 0 to area 0.
Router LSAs	Route LSA
Network LSAs	Network LSA
Summary Network LSAs	Summary network LSA
ASBR Summary LSAs	Autonomous system exterior LSA

（6）show ip ospf interface

The “show ip ospf interface” command can be used to display the OSPF protocol information for the interface.

For example, displayed information can be:

Switch#show ip ospf interface vlan 1

IP address: 11.11.4.1 Mask: 255.255.255.0 Area: 0

Net type: BROADCAST cost: 1

State: IBACKUP Type: BDR

Priority: 1 Transit Delay: 1

DR: 11.11.4.2 BDR: 11.11.4.1

Authentication key:

Timer: Hello: 10 Poll: 0 Dead: 40 Retrans: 5

Number of Neigbors: 1 Nubmer of Adjacencies: 1

Adjacencies:

1: 11.11.4.2

Displayed information	Explanation
IP address	Interface IP address
Mask	Interface mask.

Area	The area of the interface
Net type	Network type, such as broadcast, p2mp, etc.
cost	Cost value.

State	Status
Type	Layer3 switch type, such as designated layer3 switch.
Priority	Configure the priority in electing designated layer3 switch.
Transit Delay	The delay value for interface to transfer LAS.
DR	The designated layer3 switch.
BDR	Backup designated layer3 switch.
Authentication key	OSPF packet authentication key.
Timer: Hello、Poll、Dead、Retrans	OSPF protocol timer: including time set for HELLO packet, poll interval packet, route invalid, route retransmission, etc.
Number of Neigbors	The number of neighboring layer3 switches.
Nubmer of Adjacencies	The number of neighboring route interfaces.
Adjacencies	Neighboring interface IP address

（7）show ip ospf neighbor

The “show ip ospf neighbor” command can be used to display information about the neighbor OSPF layer3 switches.

For example, displayed information can be:

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1       area id 0
   router id 12.1.1.2        router ip addr 12.1.1.2
   state NFULL       priority 1
   DR 12.1.1.2        BDR 12.1.1.1
   last hello 66261       last exch 65712
interface ip 30.1.1.1       area id 0
interface ip 50.1.1.1       area id 0
   router id 50.1.1.2        router ip addr 50.1.1.2
   state NFULL       priority 0
   DR 50.1.1.1        BDR 0.0.0.0
   last hello 66286       last exch 49614
interface ip 51.1.1.1       area id 0
interface ip 52.1.1.1       area id 0
interface ip 100.1.1.1       area id 0
interface ip 110.1.1.1       area id 0
interface ip 150.1.1.1       area id 0
   router id 12.2.0.0        router ip addr 150.1.1.2
```

state NFULL priority 0
DR 150.1.1.1 BDR 0.0.0.0
last hello 66289 last exch 49607

Displayed information	Explanation
interface ip	The IP address of an interface in the current layer3 switch.

area id	The id of the area for the interface
router id	The ID of the neighbor layer3 switch.
router ip addr	The IP address of the interface in the neighbor layer3 switch.
state	Link-state status
priority	Priority.
DR	ID of the designated layer3 switch.
BDR	ID of the backup designated layer3 switch.
last hello	The last HELLO packet.
last exch	The last packet exchanged.

（8）show ip ospf routing

The “show ip ospf routing” command can be used to display information about the OSPF route table.

For example, displayed information can be:

Switch#show ip ospf routing
AS internal routes:

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
11.11.1.0	1	1	0	11.11.1.1	14.14.14.1
11.11.4.0	0	1	0	11.11.4.1	11.11.4.2
11.11.2.0	1	2	0	11.11.1.2	11.11.2.1
11.11.3.0	1	11	0	11.11.1.3	14.14.14.1

AS external routes:

Destination	Cost	Dest Type	Next Hop	ADV rtr

Displayed information	Explanation
AS internal routes	Autonomous system interior route.
AS external routes	Autonomous system exterior route.
Destination	Destination network segment
Area	Area number.
Cost	Cost value.
Dest Type	Route Type
Next Hop	Next hop
ADV rtr	Advertise the interface address of the layer3 switch.

（9）show ip ospf virtual-links

The “show ip ospf virtual-links” command can be used to display information about the OSPF virtual link.

For example, displayed information can be:

Switch#show ip ospf virtual-links

no virtual-link

（10）show ip protocols

“show ip protocols” command can be used to display the information of the routing protocols running in the switch.

For example, displayed information can be:

Switch#sh ip protocols

OSPF is running.

my router ID is 100.1.1.1

preference=10 ase perference=150

export metric=1

export tag=-2147483648

area ID 1

interface count: 2

7times spf has been run for this area

net range:

LSRefreshTime is1800

RIP information

rip is shutting down

Displayed information	Explanation
OSPF is running	The running routing protocol is OSPF protocol.
My router ID	The ID number of the layer3 switch running.
Preference	OSPF routing priority.
Ase perference	Autonomous system exterior routes priority
Export metric	Metrics for exporting OSPF routes.
Export tag	Tag value for exporting OSPF routes.
Area ID	The ID of the OSPF area that the current layer3 switch resides.
Interface count	Number of interface running OSPF routing protocol
N times spf has been run for this area	The layer3 switch performs minimum tree spanning calculation.
Net range	The network scope for running OSPF protocol.
LSRefreshTime	Link-state advertisement (LSA) update interval of OSPF protocol.

15.4.4.2 OSPF Troubleshooting Help

In configuring and using OSPF protocol, the OSPF protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

✧ Good condition of the physical connection.

- ✧ All interface and link protocols are in the UP state (use “show interface status” command).
- ✧ Then IP addresses of different network segment should be configured in all interfaces.
- ✧ Enable OSPF(use “router rip” command) first, then configure OSPF areas for appropriate interfaces to reside in.
- ✧ Next, note the nature of OSPF – OSPF backbone area (area 0) must be continuous, if not, use virtual link to make it continuous; all non-0 areas must connect to the others via area 0, direct connection between non-0 areas is not allowed; edge layer3 switch refers to the layer3 switch that partly belong to area 0 and partly belong to non-0 area; for multi-access network like broadcast network, designated layer3 switch (DR) should be elected.

15.5 Web Management

Click Route configuration. Users can configure routing protocols:

Static route configuration - Static route configuration

RIP configuration - RIP configuration

OSPF configuration - OSPF configuration

Show ip route - Show ip route

15.5.1 Static route

Click Static route configuration.

15.5.1.1 Static route configuration

Click Static route configuration. The configuration page is shown. See the equivalent CLI command at 15.2.3.2
The explanation of each field is as below:
Destination IP address - Destination IP address
Destination network mask - Destination network mask
Gateway ip – Next hop IP address
Priority – Route priority
Operation type – Add; Remove

For example: Add a route; set Destination IP address to 1.1.1.0; set Destination network mask to 255.255.255.0; set Gateway ip to 2.1.1.1; Select, and then click Apply.

Static ip route configuration	
Destination IP address	1.1.1.0
Destination network mask	255.255.255.0
Gateway ip	2.1.1.1
Priority(1-255,optional)	
Operation type	Add

15.5.2 RIP

Click RIP configuration. Users can configure RIP:

Enable RIP – Enable RIP, including:

Enable RIP – Enable RIP

Enable port to receive/transmit RIP packet – Configure the port to receive/transmit RIP packet

RIP parameter configuration – Configure RIP parameters, including:

Enable imported route – Import routes generated by other routing protocols to RIP

Metric in/out configuration – Configure metric for RIP packets received and sent through the port

RIP port imported route – RIP port imported route: sending/receiving RIP version, send/receive packet, Split-horizon status, RIP authentication

RIP mode configuration – Global RIP mode configuration: RIP version, Auto-summary, Rip priority, Rip checkzero, default metric and Rip broadcast

RIP timer configuration – Configure RIP timer

15.5.2.1 Enable RIP

Click Enable RIP. Users can enable RIP. See the equivalent CLI command at 15.3.2.2.17

The explanation of each field is as below:

Enable RIP – Enable or disable RIP

For example: Check “Enabled” box, and then click Apply.

Rip Run	
Enable RIP configuration	☑ Enabled

15.5.2.2 Port receive/transmit RIP packet configuration

Click Enable port to receive/transmit RIP packet. The configuration page is shown. See

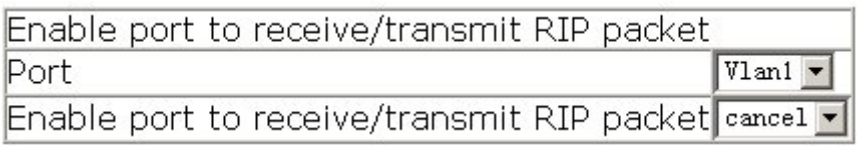
the equivalent CLI command at 15.3.2.2.11

The explanation of each field is as below:

Port – Port name

Enable port to receive/transmit RIP packet – set; cancel

For example: Disable to receive/transmit RIP packet on vlan2. Select vlan1; select vlan1; select cancel, and then click Apply.



15.5.2.3 Configuring import routes generated by other routing protocols to RIP

Import routes generated by other routing protocols to RIP

Click Enable imported route. See the equivalent CLI command at 15.3.2.2.13

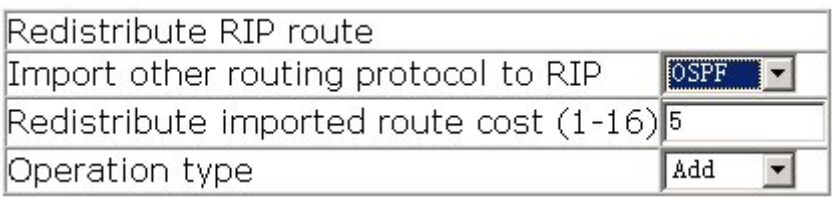
The explanation of each field is as below:

Import other routing protocol to RIP – Protocol imported: Static, OSPF and BGP

Redistribute imported route cost – Route cost

Operation type – Add or Remove

For example: Import OSPF route with cost of 5 to RIP. Set Import other routing protocol to RIP to OSPF; set Redistribute imported route cost (1-16) to 5, and then click Apply.



15.5.2.4 Port metric in/out configuration

Click Metric in/out configuration. The configuration page is shown.

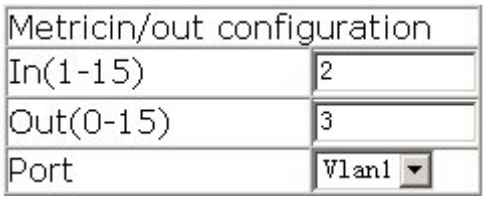
The explanation of each field is as below:

In – Metric for received RIP packets. See the equivalent CLI command at 15.3.2.2.5

Out – Metric for sent RIP packets. See the equivalent CLI command at 15.3.2.2.6

Port – Specify the port

For example: Set In to 2; set Out to 3; set Port to Vlan1, and then click Apply.



15.5.2.5 RIP port configuration

Click RIP port imported route. The configuration page is shown.

The explanation of each field is as below:

Port – Specify the port

Receiving RIP version – Configure receiving RIP version on the port: version 1, version 2 and version 1 and 2. See the equivalent CLI command at 15.3.2.2.9

Sending RIP version – Configure sending RIP version on the port: version 1, version2(BC) and version2(MC). See the equivalent CLI command at 15.3.2.2.10

Receive packet – Configure if the port is allowed to receive RIP packet: yes or no. See the equivalent CLI command at 15.3.2.2.7

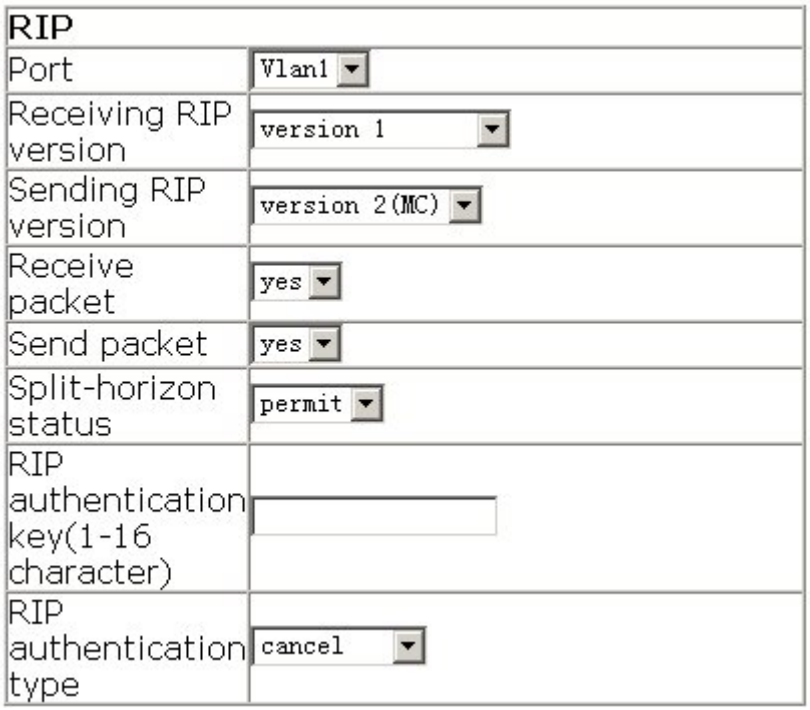
Send packet - Configure if the port is allowed to send RIP packet: yes or no. See the equivalent CLI command at 15.3.2.2.8

Split-horizon status – Configure if split-horizon is allowed on the port: permit or forbid. See the equivalent CLI command at 15.3.2.2.12

RIP authentication key – Configure RIP authentication key. See the equivalent CLI command at 15.3.2.2.3

RIP authentication type – Configure RIP authentication type: text, md5, Cisco MD5 and cancel (default type). See the equivalent CLI command at 15.3.2.2.4

For example: Set each field and then click Set.



15.5.2.6 Global RIP mode configuration

Click RIP mode configuration. The configuration page is shown.

The explanation of each field is as below:

Set receiving/sending RIP version for all ports – Configure receiving/sending RIP version for all ports: version1, version2 and Cancel (default version). See the equivalent CLI command at 15.3.2.2.19

Auto-summary – Configure auto-summary: apply and cancel: See the equivalent CLI command at 15.3.2.2.1

Rip priority(0-255) – Specify rip priority. See the equivalent CLI command at 15.3.2.2.16

Set default route cost for imported route(1-16) - Set default route cost for imported route. See the equivalent CLI command at 15.3.2.2.2

Rip checkzero – Configure RIP packet checkzero. See the equivalent CLI command at 15.3.2.2.15

Rip broadcast – Configure sending RIP broadcast and multicast packet on all the ports. See the equivalent CLI command at 15.3.2.2.14

For example: Set each field and then click Apply.

Route mode configuration	
Set receiving/sending RIP version for all ports	version 1
Auto-summary	cancel
Rip priority(0-255)	120
Set default route cost for imported route(1-16)	1
Rip checkzero	set checkzero
Rip broadcast	set

15.5.2.7 RIP timer configuration

Click RIP timer configuration. The configuration page is shown. See the equivalent CLI command at 15.3.2.2.18

The explanation of each field is as below:

Update timer – Update packet timer

Invalid timer – RIP route invalid timer

Holddown timer – Time length of a route which can stay in the route table after it is invalid.

For example: Set each field and then click Apply.

RIP	
Update timer(1-2147483647 second)	20
Invalid timer(1-2147483647 second)	80
Holddown timer(1-2147483647 second)	60

15.5.3 OSPF

Click OSPF configuration. Users can configure OSPF:

OSPF enable – Enable OSPF protocol

OSPF Tx-parameter configuration – Configure OSPF transmitting parameters

Imported route parameter configuration – Configure OSPF imported route parameters

Other parameter configuration – Configure other OSFP parameters

OSPF debug - OSPF debug information

15.5.3.1 Enable OSPF

Click OSPF enable. The configuration page is shown:

OSPF enable – Enable/disable OSPF

Router-ID configuration – Configure Router-ID for the switch

OSPF network range configuration – Configure OSPF network range

OSPF area configuration for port – Configure OSPF area for the port

15.5.3.1.1 Enable/disable OSPF

Click OSPF enable. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.19

The explanation of each field is as below:

OSPF enable - OSPF enable; OSPF disable

Reset – Clear the selection

For example: Enable OSPF protocol. Select OSPF enable, and then click Apply.



15.5.3.1.2 OSFP Router-ID configuration

Click Router-ID configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.18

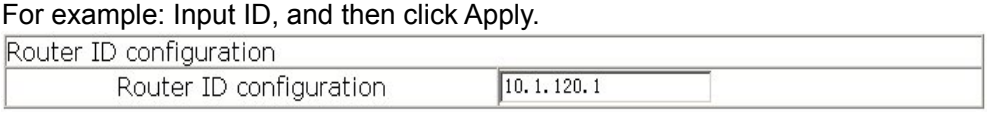
The explanation of each field is as below:

Router-ID configuration – Configure Router-ID

Reset – Reset parameter

Default – Delete Router-ID

For example: Input ID, and then click Apply.



15.5.3.1.3 OSPF network range configuration

Click OSPF network range configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.15

The explanation of each field is as below:

Network – Network IP address

Network mask - Network mask

Area ID - Area ID

Advertise – Specify if advertise the summary route: yes or no

For example: Add network range 10.1.1.0/255.255.255.0 to area 1. Set Network to 10.1.1.0; set Network mask to 255.255.255.0; set Area ID to 1; Set Advertise to yes, and then click Apply.

OSPF network range configuration	
Network	10.1.1.0
Network mask	255.255.255.0
Area ID (0-4294967295)	1
Advertise	◉ yes ○ no

15.5.3.1.4 Configure OSPF area for port

Click OSPF area configuration for port. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.9

The explanation of each field is as below:

Vlan port – Vlan port list

Area ID – Area ID

Reset – Reset

Default – Restore the default value

For example: Set the port Vlan1 to belong to area 1; Set Vlan port to Vlan1; set Area ID to 1, and then click Apply.

OSPF area configuration for port(must)	
Vlan port	Vlan1
Area ID (0-4294967295)	

15.5.3.2 OSPF transmitting parameters configuration

Click OSPF Tx-parameter configuration. Users can configure OSPF transmitting parameters:

OSPF authentication parameter configuration – Configure OSPF authentication parameter

Passive interface configuration – Set OSPF port to receive, but not to transmit

Sending packet cost configuration – Configure Sending packet cost for port

15.5.3.2.1 OSPF authentication parameter configuration

Click OSPF authentication parameter configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.6

The explanation of each field is as below:

Vlan port – Vlan port list

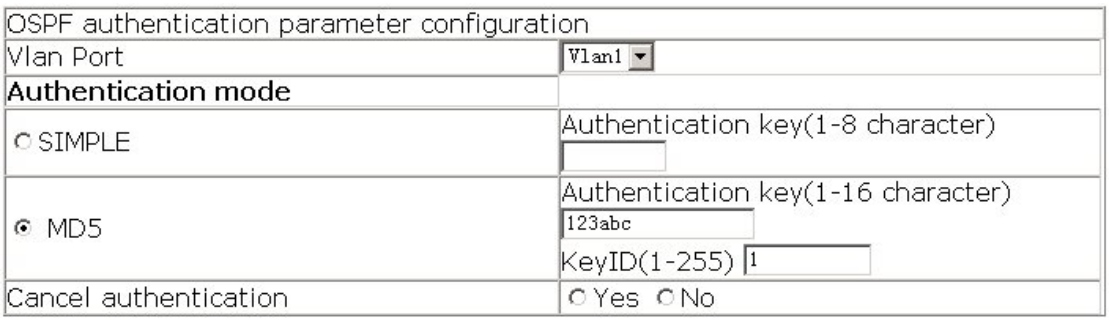
Authentication mode – Configure authentication mode: simple or MD5

Authentication key – Configure authentication key

KeyID - MD5 KeyID

Reset - Reset

For example: Set OSFP port Vlan1 to use MD5 authentication with the password of 123abc and with KeyID of 1. Select Vlan Port to Vlan1; set Authentication mode to MD5; set Authentication key to 123abc; set KeyID to 1, and then click Apply.



15.5.3.2.2 OSPF passive interface configuration

Click Passive interface configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.11

The explanation of each field is as below:

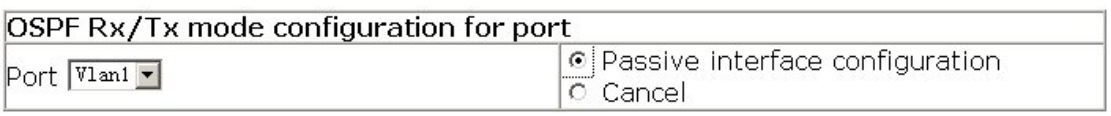
Port – Port list

Passive interface configuration – Configure passive interface

Cancel – Cancel the configuration

Reset – Restore the default value.

For example: Set vlan1 to OSFP passive interface. Set Port to Vlan1; select Passive interface configuration, and then click Apply.



15.5.3.2.3 Sending packet cost for port configuration

Click Sending packet cost configuration. The configuration page is shown.

The explanation of each field is as below:

Vlan port – Vlan port list

OSPF route cost configuration – Configure OSPF route cost. See the equivalent CLI command at 18.4.2.2.7

Hello packet interval – Specify hello packet interval on the port. See the equivalent CLI command at 15.4.2.2.10

Neighbor router invalid interval – Specify neighbor router invalid interval. See the

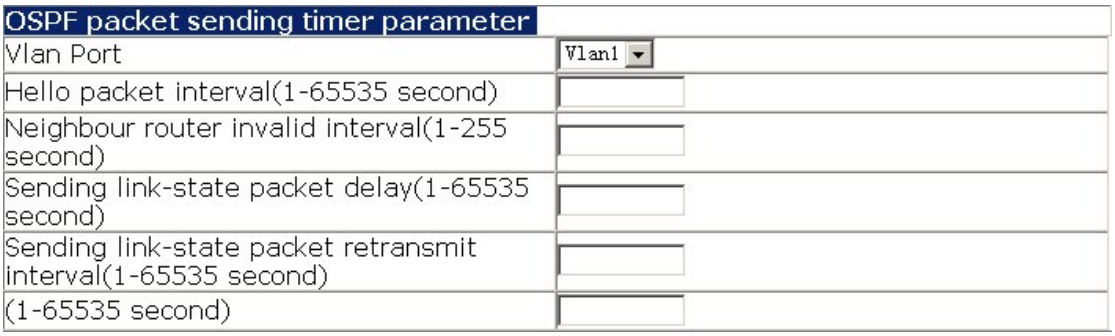
equivalent CLI command at 18.4.2.2.8

Sending link-state packet delay – Configure sending link-state packet delay on the port. See the equivalent CLI command at 18.4.2.2.14

Sending link-state packet retransmit interval – Specify sending link-state packet retransmit interval to neighbor router. See the equivalent CLI command at 15.4.2.2.13

Reset - Reset

Default - Restore the default value.



15.5.3.3 OSPF Imported route parameter configuration

Click OSPF Imported route parameter configuration. The configuration page is shown.

Imported route parameter configuration – Configure default imported route parameters

Import external routing information – Import external routing information to OSPF

15.5.3.3.1 Imported route parameter configuration

Click Imported route parameter configuration. The configuration page is shown.

The explanation of each field is as below:

Default imported route type – Set default imported route type. 1 and 2 stand for Type 1 external route and Type 2 external route. See the equivalent CLI command at 18.4.2.2.5

Default imported route tag – Configure default imported route tag. See the equivalent CLI command at 15.4.2.2.4

Default imported route cost – Configure default imported route cost. See the equivalent CLI command at 15.4.2.2.1

Importe route interval – Configure importe route interval. See the equivalent CLI command at 15.4.2.2.2

Maximum imported route – Configure maximum number of imported route. See the equivalent CLI command at 15.4.2.2.3

Imported route parameter	
Default imported route type	1
Default imported route tag(0-4294967295)	
Default imported route cost (1-65535)	
Imported route interval(1-65535)	
Maximum imported route(1-65535)	

15.5.3.3.2 Import external routing information configuration

Click Import external routing information. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.17.

The explanation of each field is as below:

Imported type – Configure imported route type: Static, RIP, connected，BGP

Type – Specify - Set default imported route type. 1 and 2 stand for Type 1 external route and Type 2 external route.

Tag – Configure route tag

Metric value – Set route metric value

Import external routing information	
Imported type	Type
static	1
Tag(0-4294967295)	
Metric Value(1-16777215)	

15.5.3.4 Other OSFP parameter configuration

Click Other parameter configuration. The configuration page is shown.

OSPF priority configuration – Configure OSPF priority

OSPF STUB area and default route cost – Configure OSPF STUB area and default route cost

OSPF virtual link configuration – Configure OSPF virtual link

Port DR priority configuration – Configure Port DR priority for port election

15.5.3.4.1 OSPF priority configuration

Click OSPF priority configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.16

The explanation of each field is as below:

ASE – “yes” sets to specify priority for imported external AS route; “no” sets to specify

OSPF priority relative to other routing protocols.

Priority – set priority value



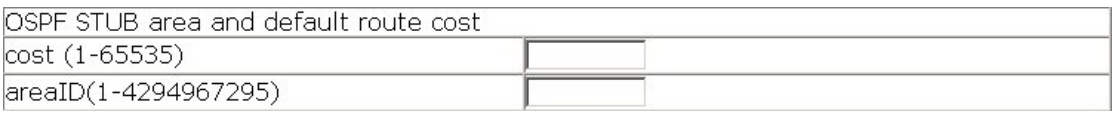
15.5.3.4.2 OSPF STUB area and default route cost configuration

Click OSPF STUB area and default route cost. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.20

The explanation of each field is as below:

Cost – Stub area default cost

areaID – Stub area ID



15.5.3.4.3 OSPF virtual link configuration

Click OSPF virtual link configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.21

The explanation of each field is as below:

router_id – Configure router_id for virtual link neighbor

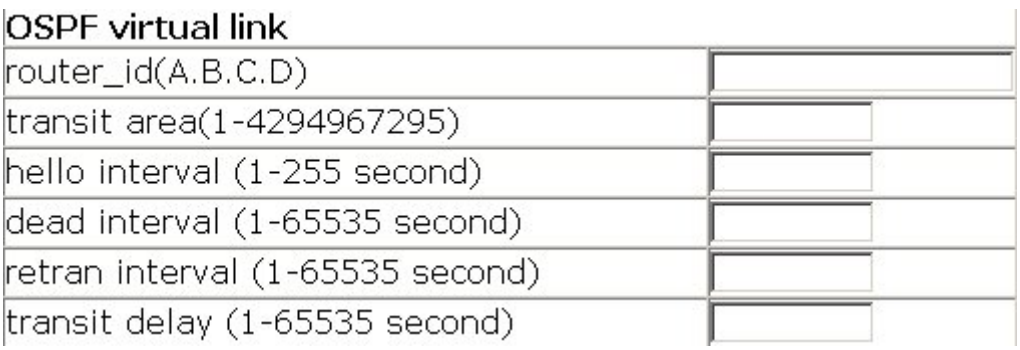
transit area – Configure transit area number

hello interval – Configure hello interval

dead interval – Configure route dead interval

retran interval – Configure retransmit interval for LSA

transit delay – Configure transit delay for LSA



15.5.3.4.4 Port DR priority configuration

Click Port DR priority configuration. The configuration page is shown. See the equivalent CLI command at 15.4.2.2.12

The explanation of each field is as below:

Vlan Port – Specify Vlan port

Priority – Specify priority



15.5.3.5 OSPF debug

Click OSPF debug. The configuration page is shown:

show ip ospf – Show OSPF information. See the equivalent CLI command at 15.4.2.2.22

show ip ospf ase – Show external AS OSPF information. See the equivalent CLI command at 15.4.2.2.23

show ip ospf cumulative – Show OSPF statistics. See the equivalent CLI command at 15.4.2.2.24

show ip ospf database – Show OSPF link state database. See the equivalent CLI command at 15.4.2.2.25

show ip ospf neighbor – Show OSFP neighbor information. See the equivalent CLI command at 15.4.2.2. 27

show ip ospf routing – Show OSFP routing table. See the equivalent CLI command at 15.4.2.2. 28

show ip ospf virtual-links – Show OSPF virtual-link information. See the equivalent CLI command at 15.4.2.2.29

show ip protocols – Show the current running routing protocols on the switch. See the equivalent CLI command at 15.4.2.2.30

Click the node to show the debug information.

15.5.3.5.1 Show ip route

Click Show ip route to show ip routing table.

Information display

```
Total route items is 1, the matched route items is 1
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived, D - DVMRP derived

  Destination      Mask            Nexthop       Interface        Preference
C  192.168.1.0      255.255.255.0    0.0.0.0       Vlan1            0
```

Chapter 16 Multicast Protocol Configuration

16.1 Multicast Protocol Overview

16.1.1 Introduction to Multicast

When sending information (including data, voice and video) to a small number of users in the network, there are several ways of transmission, for instance, the unicast method that establish a separate data transmission channel for each user or the broadcast method sending information to all users in the network regardless of whether they need the information or not. Suppose 200 users in a network need to receive the same information, traditionally, the unicast method is employed to sends the same information 200 times to ensure users requiring the data can get what they need; or the information is broadcasted throughout the network so that users requiring the data can obtain what they need directly from the network. Both two methods waste a large amount of precious bandwidth resource, and the broadcast method is unfavorable to the security of the information or keep it secret.

The advent of IP multicast technology solved this problem. Multicast source sends the information only once, and the multicast routing protocol create a tree route for the multicast packet; the information being transferred will start duplicating and distribution in the fork as far as possible. This way, the information can be sent to each user requiring it accurately and efficiently.

It should be noted that the multicast source is not necessarily a member of the multicast group. When sending data to some multicast group, the sender itself is not necessarily a receiver of that group. Multiple sources are allowed to send packets to the same multicast group at the same time. There may be routers not support multicast in the network. Multicast routers can transfer the multicast packets encapsulated in unicast IP packets in tunnel mode to the neighbor multicast routes, the neighbor multicast routers will strip the unicast IP head can continue multicast transmission. This way, large modification to the network structure can be avoided. The major benefits of multicast are:

1) Improved efficiency and reduced network traffic and server/CPU load.
2) Improved performance and reduced unnecessary traffic.
3) Distributed application: enabling multiple points application.

16.1.2 Multicast Address

The multicast packets uses Class D IP address as their destination addresses, ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot be used in the source IP address field of an IP packet. In unicast, the path a packet travels is from the source address to the destination address, and the packet is transfer in the network hop-by-hop. However, in IP multicast, the destination address of a packet is a group (group address) instead of one single address. All information receivers are arranged in the same group. And once a receiver joins a multicast group, data sending to the multicast address will immediately start transferring to the receiver. All members in the group will receive the packets. The membership for multicast group is dynamic, the hosts can join and quit a multicast group at any time.

A multicast group can be either a perpetual one or temporary one. Part of multicast addresses are assigned officially and referred to as the perpetual multicast group. The IP address of a perpetual multicast group remains the same, but the membership can be changed. A perpetual multicast group can have any number of members, even zero. The IP multicast addresses not reserved for perpetual multicast group can be used by temporary multicast groups.

224.0.0.0 – 224.0.0.255 are reserved multicast addresses (perpetual group address), the address 224.0.0.0 is not used, the other addresses are available for routing protocols; 224.0.1.0 – 238.255.255.255 are multicast addresses available to users (temporary group address), and is valid for the whole network; 239.0.0.0 – 239.255.255.255 are local administrative multicast address and is valid for specific local ranges. The following is a list for common reserved multicast addresses:

224.0.0.0 Base address (reserved)

224.0.0.1 All-host address

224.0.0.2 All-multicast-router address

224.0.0.3 Not for allocation

224.0.0.4 DVMRP router

224.0.0.5 OSPF router

224.0.0.6 OSPF DR

224.0.0.7 ST router

224.0.0.7 ST host

224.0.0.9 RIP-II router

224.0.0.10 IGRP router

224.0.0.11 Active proxy

224.0.0.12 DHCP Server/Relay proxy

224.0.0.13 All PIM routers

224.0.0.14 RSVP packaging

224.0.0.15 All CBT routers

224.0.0.16 Specified SBM

224.0.0.17 All SBMS

224.0.0.18 VRRP

When transferring unicast IP packets on Ethernet, the destination MAC address is the MAC of the receiver. However, in transferring multicast packets, as the destination is no longer one specific recipient but a group with unknown members, the destination address used Is the multicast MAC address. Multicast MAC address is corresponding 5to the multicast IP address. According to IANA (Internet Assigned Number Authority), the 24 MSbs of multicast MAC is 0x01005e and 23 LSbs of multicast MAC is the same of the multicast IP address.

As only 23 bits out of the 28 LSbs of multicast IP address are mapped to MAC address, for one MAC address there will be 32 corresponding multicast IP addresses.

16.1.3 IP Multicast Packets Forwarding

In the multicast model, the source host sends information to the host group represented by the multicast group address in the destination address field of the IP packet. The multicast model differs from the unicast model in that a multicast packet must be forwarded to several external interfaces to send the packet to all receiving stations, i.e. multicast forwarding is more complex than unicast forwarding.

To ensure the multicast packets reach the routers in the shortest route, the multicast protocols must check the receiving interfaces of the multicast packets against the unicast route table or route table dedicated for multicast (such as a DVMRP route table). Such check mechanism is the base for most multicast routing protocols to perform forwarding, and is called Reverse Path Forwarding (RPF) check. Multicast routers use the source address of an arrived multicast packet to query the unicast route table or an independent multicast route table to make sure the ingress interface at which packet arrived is in the shortest route from the receiving station to the source address. If an active tree is used, the source address is the address of source host sending the multicast packet; if a shared tree is used, the source address is the root address of that shared tree. When a multicast packet arrives at a router, the packet will be forwarded according to the multicast forwarding rules if the RPF check ok; otherwise, the packet will be discarded.

16.1.4 Application of Multicast

IP multicast technology effectively solved the problem of one sender vs. multiple receivers, fulfilling the high efficiency data transmission from one point to multiple points in the IP

network, and can significantly save the network bandwidth and reduce network traffic. The multicast feature can be conveniently used to provide some new value-added services, including online live broadcast, network TV, remote education, remote medical service, network radio, realtime video/audio meeting that can be summarized in the following three fields:

1) Multimedia and stream application.
2) Data warehouse and financial (like stocks) application.
3) Any point-to-multiple-points data distribution application.

With the increasing of multimedia services in the IP network, multicast represents great market potential, and multicast service is spreading quickly and widely used.

16.2 Common Multicast Configurations

16.2.1 Common Multicast Configuration Commands

- **show ip mroute**

16.2.1.1 show ip mroute

Command: show ip mroute [*group_address*] [*source_address*]
Function: Display the IP multicast packet forwarding entries..
Parameter: [*group_address*] specifies the group address for the forwarding entry to be displayed; **[*source_address*]** specifies the source address for the forwarding entry to be displayed
Default: No display by default.
Command mode: Admin Mode
Usage Guide: This command is used to display IP multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.
Example: Display all IP multicast forwarding entries.

```
Switch # show ip mroute
Name: Loopback, Index: 2001, State: 9 localaddr: 127.0.0.1, remote: 127.0.0.1
Name: Vlan1, Index: 2005, State: 13 localaddr: 1.1.1.1, remote: 1.1.1.1
Name: Vlan4, Index: 2006, State: 13 localaddr: 2.1.1.1, remote: 2.1.1.1
Name: Vlan3, Index: 2007, State: 13 localaddr: 3.1.1.1, remote: 3.1.1.1
Group            Origin          Iif          Wrong   Oif: TTL
225.1.1.101      1.1.1.100       Vlan1          0       2006: 1
                                                        2007: 1
239.255.0.1      9.1.1.100       Vlan4          0       2005: 1
```

239.255.0.1 7.1.1.100 Vlan4 0 2005: 1
239.255.0.1 1.1.1.100 Vlan1 0 2006: 1
2007: 1

Switch #

Displayed information	Explanation
Name	The interface list used by the multicast protocol and basic information for the interfaces.
Index	Index number for the interface
Group	Multicast forwarding entry group address
Origin	Multicast forwarding entry source address
Iif	Multicast forwarding entry ingress interface
Wrong	The number of multicast packets (to this forwarding entry) from wrong incoming interfaces
Oif: TTL	Oif stands for the outgoing interface list, this list can be referred to by the index number according to the information list above; TTL is the TTL threshold value for that outgoing interface.

16.3 PIM-DM

16.3.1 Introduction to PIM-DM

PIM-DM (Protocol Independent Multicast Dense Mode) is a dense mode multicast protocol. It is good for use in small networks as the multicast group members are relatively concentrated in such network environment.

The work process of PIM-DM can be summarized as the following phases: neighbor discovery, flooding & prune, grafting.

1. Neighbor discovery

PIM-DM routers need to discover the neighbors with HELLO packets on start up. Network nodes running PIM-DM keeps contact with HELLO packets. The HELLO packets are sent in regular intervals.

2. Flooding and Prune

PIM-DM assumes all hosts in the network are ready for receiving multicast data. When a multicast source S starts sending data to multicast group G, the router will first perform RPF check against the unicast route table to the multicast packet. If checked ok, the router will create a (S, G) entry and forward the multicast packet to all downstream PIM-DM nodes in the network (Flooding). If RPF check fails, indicating the multicast packet is coming from the wrong interface, the packet will be discarded. After this process, each node in the PIM-DM multicast domain will create a (S, G) entry. If no multicast group member exists in the downstream nodes, then a prune message will be sent to the

upstream nodes to inform the upstream node that no more forwarding for that multicast group is necessary. The upstream nodes will delete the corresponding interface, multicast forwarding entry(S,G), from the outgoing interface list. Hence a shortest path tree (SPT) rooted by source S is established. The prune process is initiated by leaf routers first.

The above procedures are referred to as the Flooding-Prune process. A timeout mechanism is provided for each pruned nodes, when the prune timeout, the route restart the flooding-prune process. The PIM-DM flooding-prune process is performed in regular intervals.

3. RPF check

PIM-DM employs the RPF check method to build a multicast tree rooted from the data source according to the existing unicast route table. When a multicast arrives at the router, its path correctness is checked first. If as indicated by the unicast route, the arriving interface is the interface to the multicast source, the packet is considered to be from the correct path; otherwise, the multicast packet is discarded as a redundant packet. The unicast route information used as the route decision fact is not dependent on specific unicast routing protocol, but can be the route information of any unicast routing protocols, such as route discovered by RIP, OSPF, etc.

4. Assert mechanism

If two routes (A and B) in the same LAN segment both have a receiving path to multicast source S, both will forward the multicast packet sent by multicast source S in the LAN. As a result, the downstream multicast router C will receive two identical multicast packets. On detecting such situation, the router will decide a unique forwarder through the Assert mechanism. The best forwarding path is decided by sending Assert packets. If two or more paths have the same priority and costs, then the node with a larger IP address is selected as the upstream neighbor for the (S, G) entry and is responsible for the forwarding of multicast packet for that (S, G) entry,.

5. Graft

If a pruned downstream node needs to restore to the forwarding state, the node will send a graft packet to ask the upstream to restore multicast data forwarding.

16.3.2 PIM-DM Configuration

16.3.2.1 PIM-DM Configuration Task Sequence

1、 Enable PIM-DM (required)

2、 Configure PIM-DM sub-parameters (optional)

Configure PIM-DM interface parameters

Configure PIM-DM HELLO packet interval

1. Enable PIM-DM

Basic configuration of PIM-DM routing protocol on route switch is quite simple: just enable

PIM-DM in the appropriate interfaces.

Command	Explanation
Interface Mode	
ip pim dense-mode **no ip pim dense-mode**	Enable PIM-DM protocol; the "**no ip pim dense-mode**" command disables PIM-DM protocol (required)

2. Configure PIM-DM sub-parameters

Configure PIM-DM interface parameters

a. Configure PIM-DM HELLO packet interval

Command	Explanation
Interface Mode	
ip pim hello-interval **<hello-interval-seconds>** **no ip pim hello-interval**	Set interval for sending PIM-DM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

3. Disable PIM-DM protocol

Command	Explanation
Interface Mode	
no ip pim dense-mode	Disable PIM-DM protocol

16.3.2.2 PIM-DM Configuration Commands

- **ip pim dense-mode**
- **ip pim hello-interval**
- **show ip pim interface**
- **show ip pim mroute dm**
- **show ip pim neighbor**
- **debug ip pim**

16.3.2.3 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enable PIM-DM protocol on the interface; the "**no ip pim dense-mode**"

command disables PIM-DM protocol on the interface.

Parameter: N/A.

Default: PIM-DM protocol is disabled by default.

Command mode: Interface Mode

Usage Guide:

Example: Enable PIM-DM protocol on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim dense-mode

16.3.2.4 ip pim hello-interval

Command: ip pim hello-interval <*hello-interval-seconds*>

no ip pim hello-interval

Function: Set interval for sending PIM-DM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

Parameter: < ***hello-interval-seconds*** > is the interval for sending PIM-DM HELLO packets, ranging from 1 to 18724s.

Parameter: The default interval for sending PIM-DM HELLO is 10s.

Command mode: Interface Mode

Usage Guide: The HELLO message enable PIM-DM switches to locate each other and establish the neighborhood. PIM-DM switches claim their existence by sending HELLO message to their neighbors. If no HELLO message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time must be no greater than the neighbor timeout time.

Example: Configure PIM-DM HELLO interval on interface vlan1.

Switch (Config)#interface vlan1

Switch(Config-If-Vlan1)#ip pim hello-interval 20

16.3.3 Typical PIM-DM Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and PIM-DM protocol is enabled on each vlan interface.

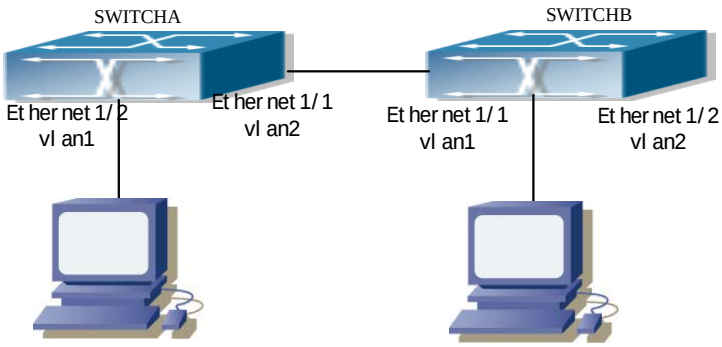


Fig 16-1 Typical PIM-DM environment

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SwitchA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim dense-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan2

Switch(Config-If-Vlan1)# ip pim dense-mode

(2) Configuration of SwitchB:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim dense-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan1)# ip pim dense-mode

16.3.4 PIM-DM Troubleshooting Help

1. Monitor and Debug Commands
2. PIM-DM Troubleshooting Help

16.3.4.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip pim mroute dm	Display the PIM-DM packet forwarding entry
show ip pim neighbor	Display PIM-DM neighbor information

show ip pim interface	Display PIM-DM interface information
debug ip pim	Enable the debug function for displaying detailed PIM information; the "**no**" format of this command disables this debug function.

16.3.4.1.1 show ip pim mroute dm

Command: show ip pim mroute dm

Function: Display the PIM-DM packet forwarding entry

Parameter: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: This command is used to display PIM-DM multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example: Display all PIM-DM packet forwarding entries.

```
Switch#sh ip pim mroute dm

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
        Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
        Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

PIMDM Group Table, inodes 7 routes 4:

(5.1.1.100, 225.0.0.1), protos: 0x8, flags: 0x4, 00: 22: 21/00: 03: 30
  Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
  Outgoing interface list:
        (Vlan1), protos: 0x2, UpTime: 00: 22: 21, Exp: /
  Prune interface list:
        (Vlan2), protos: 0x2, UpTime: 00: 22: 21, Exp: 00: 03: 07

(5.1.1.100, 225.0.0.2), protos: 0x8, flags: 0x4, 00: 18: 52/00: 03: 30
  Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
  Outgoing interface list:
        (Vlan1), protos: 0x2, UpTime: 00: 18: 52, Exp: /
  Prune interface list:
        (Vlan2), protos: 0x2, UpTime: 00: 18: 52, Exp: 00: 02: 51
Switch#
```

Displayed information	Explanation
(5.1.1.100, 225.0.0.1)	Forwarding entry.
Incoming interface	Incoming interface or RPF interface.
Outgoing interface list	Outgoing interface list.
Prune interface list	Downstream prune interface list.

16.3.4.1.2 show ip pim neighbor

Command: show ip pim neighbor [<*ifname*>]

Function: Display information for neighbors of the PIM interface.

Parameter: <*ifname*> is the interface name, i.e. display PIM neighbor information of the specified interface.

Default: PIM neighbor information is displayed by default on all interfaces.

Command mode: Admin Mode

Usage Guide: If no interface name is specified, then neighbor information for all interfaces will be displayed.

Example: Display neighbor information for all interfaces (do not specify the interface name)

```
Switch#sh ip pim neighbor
Neighbor-Address Interface      ifIndex Uptime     Expires    DR-state
 2.1.1.1         Vlan1          2005    00: 25: 17 00: 01: 15 /
 9.1.1.6         Vlan2          2006    00: 25: 09 00: 01: 35 DR
 5.1.1.4         Vlan3          2007    00: 25: 01 00: 01: 38 DR
Switch#
```

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The neighbor interface discovered.
ifIndex	Interface index number
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.
DR-state	Whether the neighbor is a DR.

16.3.4.1.3 show ip pim interface

Command: show ip pim interface [<*ifname*>]

Function: Display information for the PIM interface.

Parameter: ***<ifname>*** is the interface name, i.e. display PIM information of the specified interface.

Default: PIM information is displayed by default on all interfaces.

Command mode: Admin Mode

Example: Display PIM information of interface vlan 1.

```
Switch#sh ip pim interface vlan 1
Interface Vlan1 : 2.1.1.2
  owner is pimdm, Vif is 1, Hello Interval is 30
  Neighbor-Address Interface        Uptime     Expires
  2.1.1.1          Vlan1            00: 26: 23 00: 01: 39
Switch#
```

Displayed information	Explanation
Interface (the former)	Interface name and interface IP.
Owner	Multicast routing protocol of the interface.
Vif	Corresponding virtual interface index to the interface.
Hello Interval	The HELLO packet interval configured on the interface (in seconds)
Neighbor-Address	Neighbor address
Interface (the latter)	The neighbor interface discovered.
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.

16.3.4.1.4 debug ip pim

Command: debug ip pim

Function: Enable the debug function for displaying detailed PIM information; the "**no**" format of this command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about PIM packets etc is required, this debug command can be used.

Example:

```
Switch # debug ip pim
00: 15: 45: PIM: Send v2 Hello on vlan1, holdtime 105
00: 15: 45: PIM: Send v2 Hello on vlan1, holdtime 105
00: 15: 45: PIM: Received v2 Hello on vlan1 from 2.1.1.2, holdtime 105
```

16.3.4.2 PIM-DM Troubleshooting Help

In configuring and using PIM-DM protocol, the PIM-DM protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interfaces status” command).
- ✧ Next, enable PIM-DM protocol on the interface (use the “ip pim dense-mode” command).
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured.

16.4 PIM-SM

16.4.1 Introduction to PIM-SM

PIM-SM (Protocol Independent Multicast Sparse Mode) is a sparse mode multicast protocol, the mode is protocol independent. It is mainly used in large scale networks with group members relatively scattered in large ranges. In contrast to the flooding-prune method in dense mode, PIM-SM protocol assumes no hosts are receiving the multicast packets, PIM-SM routers will send multicast packets to a host only when the host explicitly request for the packets.

By setting rendezvous points (RP) and bootstrap routers, PIM-SM announces multicast information to all PIM-SM routers and builds up RP-rooted shared tree with the router join/prune information. As a result, the bandwidth occupied by data packets and control packets can be reduced, and router processing overhead can be lowered. Multicast data move along the shared tree to the network segments of the multicast group members. When the data traffic reaches a certain level, the multicast stream can be toggled to source-based shortest path tree to reduce network lag. PIM-SM is independent of specific unicast routing protocol, but use the existing unicast routing table for RPF check.

1. How PIM-SM works

PIM-SM workflow is mainly comprised of the following parts: neighbor discovery, RP shared tree generation, multicast source registration and SPT toggle, etc. The neighbor discovery mechanism is the same as PIM-DM and is omitted here.

(1) RP shared tree (RPT) generation

When a host joins a multicast group G, the leaf route directly connected with the host learns the presence of recipient of multicast group G through IGMP packets. The router then calculates the corresponding rendezvous point (RP) for the multicast group G, and

sends a join message to the upstream node in the RP direction. Each routers between the leaf router and the RP will created a (*, G) entry in their forwarding table, indicating packets sent by any source to multicast group G applies to this entry. When RP receives a packet sending to multicast group G, the packet will move along the established route to reach the leaf router and the host. This completes a RP-rooted RPT.

(2) Multicast source registration.

When multicast source S sends a multicast packet to multicast group G, the PIM-SM multicast router directly connected to it will packet the multicast packet as a registration packet and unicast to the appropriate RP. If multiple PIM-SM multicast routers exist in the network, the designated router (DR) is responsible for the forwarding of this multicast packet.

(3) SPT toggle

When multicast router finds the multicast packets from RP destined to G in a speed exceeding the threshold, the multicast router will send a join message to the upstream node in the source S direction and cause the toggling from RPT to SPT.

2. Pre-PIM-SM configuration work

(1) Configure candidate RP

In PIM-SM networks, multiple RPs are allowed, they are referred to as the candidate RP (C-RP). Each C-RP is responsible for the forwarding of multicast packet destined to a certain range of addresses. Configuring multiple C-RP enables RP load balance. All C-RPs are of the same priority. On receiving BSR advertised C-RP message, multicast routers will calculate the RP corresponding to a certain multicast group with a same algorithm.

It should be noted that one RP can service multiple multicast groups or all multicast groups. Each multicast group in any time can have only one corresponding RP, multiple association is forbidden.

2) Configure BSR

BSR is the core of management in PIM-SM networks; it is responsible for gathering information from C-RP and broadcasting the information gathered.

Each network can have one BSR, and several Candidate-BSRs (C-BSRs). This way, once a BSR fails, another BSR will quickly take its place. BSR will be decided by the auto-election between C-BSRs.

16.4.2 PIM-SM Configuration

16.4.2.1 PIM-SM Configuration Task Sequence

1. Enable PIM-SM (required)
2. Configure PIM-SM sub-parameters

(1) Configure PIM-SM interface parameters

1） Configure PIM-SM HELLO packet interval

2） Configure a interface as the PIM-SM area border

(2) Configure PIM-SM global parameters

1) Configure a switch as the candidate BSR.

2) Configure a switch as the candidate RP.

3. Disable PIM-SM protocol

1. Enable PIM-SM protocol

Basic configuration of PIM-SM routing protocol on Route switch is quite simple: just enable PIM-SM in the appropriate interfaces.

Command	Explanation
Interface Mode	
ip pim sparse-mode **no ip pim sparse-mode**	Enable PIM-SM protocol; the "**no ip pim sparse-mode**" command disables PIM-SM protocol (required)

2. Configure PIM-SM sub-parameters

1) Configure PIM-SM interface parameters

1） Configure PIM-SM HELLO packet interval

Command	Explanation
Interface Mode	
ip pim hello-interval ***<hello-interval-seconds>*** **no ip pim hello-interval**	Set interval for sending PIM-SM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

2) Configure the interface as the PIM-SM BSR border

Command	Explanation
Interface Mode	
ip pim bsr-border **no ip pim bsr-border**	Set the interface as the PIM-SM BSR border; the "**no ip pim bsr-border**" command cancels the setting of BSR border.

2) Configure PIM-SM global parameters

1) Configure a switch as the candidate BSR.

Command	Explanation
Interface Mode	

ip pim bsr-candidate <*ifname*> [*hashlength*] [*Priority*] **no ip pim bsr-candidate**	This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to comtend for the BSR router with the other candidate BSRs; the "**no ip pim bsr-candidate**" command cancels the BSR configuration.

2) Configure a switch as the candidate RP.

Command	Explanation
Interface Mode	
ip pim rp-candidate <*ifname*> [group-list *access-list*] [interval *interval*] **no ip pim rp-candidate [<*ifname*>]**	This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to comtend for the RP router with the other candidate RPs; the "**no ip pim rp-candidate [<*ifname*>]**" command cancels the RP configuration.

3. Disable PIM-SM protocol

Command	Explanation
Interface Mode	
no ip pim sparse-mode	Disable PIM-SM protocol

16.4.2.2 PIM-SM Configuration Commands

- **ip pim sparse-mode**
- **ip pim bsr-border**
- **ip pim hello-interval**
- **ip pim bsr-candidate**
- **ip pim rp-candidate**
- **show ip pim bsr-router**
- **show ip pim interface**
- **show ip pim mroute sm**
- **show ip pim neighbor**
- **show ip pim rp**
- **debug ip pim**
- **debug ip pim bsr**

16.4.2.2.1 ip pim sparse-mode

Command: ip pim sparse-mode
no ip pim sparse-mode

Function: Enable PIM-SM protocol on the interface; the "**no ip pim sparse-mode**" command disables PIM-SM protocol on the interface.

Parameter: N/A.

Default: PIM-SM protocol is disabled by default.

Command mode: Interface Mode

Example: Enable PIM-SM protocol on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim sparse-mode

16.4.2.2.2 ip pim bsr-border

Command: ip pim bsr-border
no ip pim bsr-border

Function: This command is the configuration command for interface BSR border. It is used to configure the border for PIM-SM area to prevent BSR message flooding outside the local PIM-SM area; the "**no ip pim bsr-border**" command cancels the BSR border configuration.

Parameter: N/A.

Default: BSR border configuration on interfaces is disabled by default.

Command mode: Interface Mode

Usage Guide: This command is the configuration commands for interface BSR border. It is used to configure the border for PIM-SM area to prevent BSR message flooding outside the local PIM-SM area. In other words, BSR messages inside the local PIM-SM area cannot be transferred from this interface to the outside; to cancel the setting of BSR border, the configuration of this command should be reverted.

Example: Enable BSR border setting on interface vlan 1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim bsr-border

16.4.2.2.3 ip pim hello-interval

Command: ip pim hello-interval <*hello-interval-seconds*>
no ip pim hello-interval

Function: Set interval for sending PIM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

Parameter: <***hello-interval-second***> is the interval for sending PIM HELLO packets, ranging from 1 to 18724s.

Parameter: The default interval for sending PIM HELLO is 30s.

Command mode: Interface Mode

Usage Guide: The HELLO message enables PIM-DM switches to locate each other and establish the neighborhood. PIM-DM switches claim their existence by sending HELLO message to their neighbors. If no HELLO message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time must be no greater than the neighbor timeout time.

Example: Configure PIM-SM HELLO interval on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim hello-interval 20

16.4.2.2.4 ip pim bsr-candidate

Command: ip pim bsr-candidate <*ifname*> [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to comtend for the BSR router with the other candidate BSRs; the "**no ip pim bsr-candidate**" command cancels the BSR configuration.

Parameter: ***ifname*** is the name of the specified interface; **[*hash-mask-length*]** is the mask length of the specified hash algorithm used in RP boot selection, ranging from 0 to 32; **[*priority*]** is the BSR priority of this candidate BSR, ranging from 0 to 255, if this parameter is omitted, the priority of this candidate BSR will be defaulted to 0.

Default: The switch is not BSR candidate router by default.

Command mode: Global Mode

Usage Guide: : This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to comtend for the BSR router with the other candidate BSRs. The switch will be a BSR candidate router only when this command is configured.

Example: Set the interface vlan1 as the BSR message sending interface.

Switch (Config)# ip pim bsr-candidate vlan1 30 10

16.4.2.2.5 ip pim rp-candidate

Command: ip pim rp-candidate <ifname> [group-list access-list] [interval interval]

no ip pim rp-candidate [<*ifname*>]

Function: This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to comtend for the RP

router with the other candidate RPs; the "**no ip pim rp-candidate [<*ifname*>]**" command cancels the RP configuration.

Parameter: <*ifname*> is the name of specified interface; ***access-list*** is the number of group range list can be used as the RP in the switch, ranging from 1 to 99, if this parameter is omitted, the router can work as the RP for all multicast groups; ***interval*** is the interval for the local candidate RP to send C-RP packets, ranging from 1 to 16383 seconds.

Default: The switch is not BSR candidate router by default.

Command mode: Global Mode

Usage Guide: This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to comtend for the RP router with the other candidate RPs. The switch will be a RP candidate router only when this command is configured.

Example: Set the interface vlan1 as the candidate RP announcing message sending interface.

```
Switch (Config)# ip pim rp-candidate vlan1 group-list 5
Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255
```

16.4.3 Typical PIM-SM Scenario

As shown in the figure below, the Ethernet interfaces of SWITCHA, SWITCHB, SWITCHC and SWITCHD are added to the appropriate vlan, and PIM-SM protocol is enabled on each vlan interface.

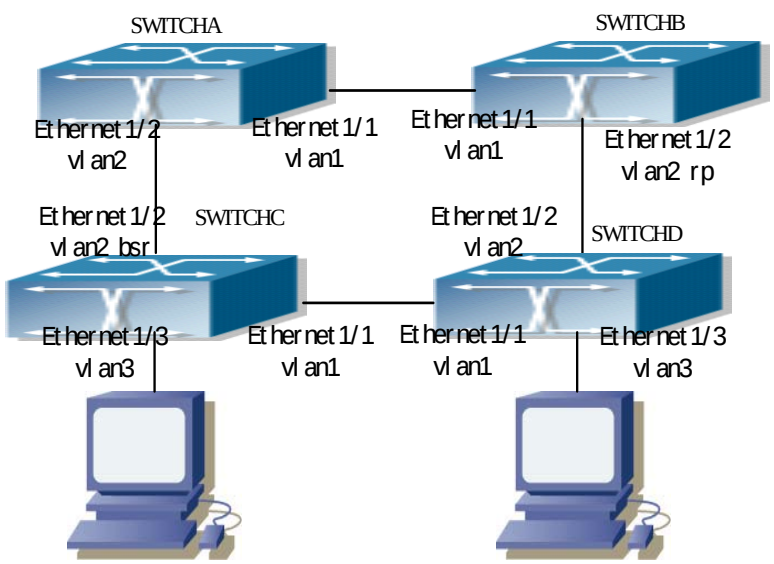


Fig 16-2 Typical PIM-SM environment

The followings are the configurations of SWITCHA, SWITCHB, SWITCHC, and SWITCHD.

(1) Configuration of SWITCHA:

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
```

(2) Configuration of SWITCHB:

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch (Config)# ip pim rp-candidate vlan2 group-list 5
Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255
```

(3) Configuration of SWITCHC:

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (Config)# ip pim bsr-candidate vlan2 30 10
```

(4) Configuration of SWITCHD:

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
```

Switch(Config-If-Vlan3)# ip pim sparse-mode

16.4.4 PIM-SM Troubleshooting Help

16.4.4.1 Monitor and Debug Commands

16.4.4.1.1 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Display pim bsr-router information.

Parameter: N/A.

Default: No display by default.

Command mode: Admin Mode

Example: Display pim bsr-router information.

Switch #show ip pim bsr-router

Switch #

PIMv2 Bootstrap information

BSR address: 192.4.1.3

Priority: 192, Hash mask length: 30

Expires : 00: 02: 13.

Switch #

Displayed information	Explanation
BSR address	Bsr-router address
Priority	Bsr-router priority
Hash mask length	Bsr-router hash mask length
Expires	The remaining time before considering the Bsr-router to be invalid.

16.4.4.1.2 show ip pim interface

Command: show ip pim interface [<*ifname*>]

Function: Display information for the PIM interface.

Parameter: <*ifname*> is the interface name, i.e. display PIM information of the specified interface.

Default: No display by default.

Command mode: Admin Mode

Function: Display PIM information of interface vlan 2.

Switch #show ip pim interface vlan2

Switch #

Interface Vlan2 : 192.3.1.2

owner is pimsm, Vif is 1, Hello Interval is 30, pim sm jp interval is (60)

Neighbor-Address Interface Uptime Expires

192.3.1.3 Vlan2 00: 12: 18 00: 01: 38

Switch #

Displayed information	Explanation
Interface (the former)	Interface name and interface IP.
owner	Multicast routing protocol of the interface.
Vif	Corresponding virtual interface index to the interface.
Hello Interval	The HELLO packet interval configured on the interface (in seconds)
jp interval	Join/prune interval.
Neighbor-Address	Neighbor address
Interface (the latter)	The neighbor interface discovered.
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.

16.4.4.1.3 show ip pim mroute sm

Command: show ip pim mroute sm

Function: Display the PIM-SM packet forwarding entry

Parameter: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: This command is used to display PIM-SM multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example:

Switch # show ip pim mroute sm

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;

Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;

Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

PIMSM Group Table, inodes 1 routes 1:

(192.1.1.1, 225.0.0.1), protos: 0x8, flags: 0x0, 00: 10: 18/00: 03: 18

Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 0
Outgoing interface list:
(Vlan2), protos: 0x2, UpTime: 00: 10: 18, Exp: 00: 03: 18
Switch #

Displayed information	Explanation
(192.1.1.1, 225.0.0.1)	Forwarding entry.
Incoming interface	Incoming interface, or RPF interface.
Outgoing interface list	Outgoing interface list.

16.4.4.1.4 show ip pim neighbor

Command: show ip pim neighbor [<*ifname*>]

Function: Display information for neighbors of the PIM interface.

Parameter: <*ifname*> is the interface name, i.e. display PIM neighbor information of the specified interface.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: If no interface name is specified, then neighbor information for all interfaces will be displayed.

Example: Display neighbor information for all interfaces (do not specify the interface name)

Switch # show ip pim neighbor

Neighbor-Address	Interface	ifIndex	Uptime	Expires	DR-state
192.3.1.3	Vlan1	28	00: 11: 39	00: 01: 16	DR
192.2.1.1	Vlan2	31	00: 11: 39	00: 01: 16	/
192.4.1.4	Vlan4	33	00: 11: 39	00: 01: 44	DR
192.4.1.3	Vlan4	33	00: 11: 39	00: 01: 17	/

Switch #

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The neighbor interface discovered.
ifIndex	Interface index number
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.
DR-state	Whether the neighbor is a DR.

16.4.4.1.5 show ip pim rp

Command: show ip pim rp [mapping | *group-address*]

Function: Display PIM RP related information

Parameter: mapping displays the group address and RP association.

group-address is the group address.

Default: No display by default.

Command mode: Admin Mode

Function: Display the RP information for PIM area 226.1.1.1.

Switch #show ip pim rp 226.1.1.1

RP Address for this group is: 192.2.1.1

Displayed information	Explanation
RP Address	RP address of the group.

16.4.4.1.6 debug ip pim

Command: debug ip pim

Function: Enable the debug function for displaying detailed PIM information; the "**no**" format of this command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about PIM packets etc is required, this debug command can be used.

Example:

Switch # debug ip pim

PIM debug is on

00: 17: 52: PIM: Received v2 Join/Prune on Vlan2 from 192.3.1.3 to 192.3.1.2

00: 17: 52: PIM: Receive Join-list: (192.1.1.1/32, 225.0.0.1/32), S-bit set

00: 17: 54: PIM: Received v2 Hello on Vlan4 from 192.4.1.4, holdtime 105

00: 17: 57: PIM: Received v2 Hello on vlan3 from 192.2.1.1, holdtime 105

00: 17: 57: PIM: Received v2 Hello on Vlan2 from 192.3.1.3, holdtime 105

00: 17: 58: PIM: Received v2 Hello on Vlan4 from 192.4.1.3, holdtime 105

00: 18: 21: PIM: Send v2 Hello on vlan2, holdtime 105

00: 18: 21: PIM: Send v2 Hello on vlan4, holdtime 105

00: 18: 21: PIM: Send v2 Hello on vlan3, holdtime 105

00: 18: 21: PIM: Send v2 Hello on Vlan4, holdtime 105

00: 18: 21: PIM: Send v2 Hello on Vlan2, holdtime 105

16.4.4.1.7 debug ip pim bsr

Command: debug ip pim bsr

Function: Enable the PIM candidate RP/BSR informaiton debug function; the "**no**" format of the command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about PIM candidate RP/BSR packets, etc. is required, this debug command can be used.

Example:

Switch # debug ip pim bsr

PIM BSR debug is on

00: 16: 23: PIM: Received v2 BSR on Vlan4 from 192.4.1.3

00: 16: 23: PIM: Receive BSR fragtag 6879, hmlen: 30, pri: 192

00: 16: 23: PIM: Receive BSR Group (225.0.0.1, 0.0.0.0): rpcount: 1, fragcount: 1

00: 16: 23: PIM: C-RP 192.2.1.1, holdtime 130, C-RP pri 192

00: 16: 23: PIM: Transmit the BSR message on Vlan2

00: 16: 23: PIM: Transmit the BSR message on vlan4

00: 16: 23: PIM: Transmit the BSR message on vlan3

00: 16: 23: PIM: Transmit the BSR message on vlan2

16.4.4.2 PIM-SM Troubleshooting Help

In configuring and using PIM-SM protocol, the PIM-SM protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interfaces status" command).
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured.
- ✧ PIM-SM protocol requires the support of RP and BSR. So "**show ip pim bsr-router**" command should be run first for BRS information, if no BSR exists, then unicast route to BSR should be checked.
- ✧ Use the "**show ip pim rp**" command to verify RP information is correct. If no RP information is displayed, unicast route should be checked, too.

16.5 DVMRP

16.5.1 Introduction to DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a dense mode multicast routing protocol. It employs a RIP like route exchange mechanism to establish a forwarding broadcast tree for each source, then a truncated broadcast tree (short path tree to the source) will be created by dynamic pruning/grafting. Reverse path forwarding (RPF) is used to decide whether multicast packet should be forwarded to the downstream nodes.

The following are some important DVMRP features:

1. The route exchange process determining RPF information is based on distance vectors (in the way similar to RIP)
2. Route exchange occurs periodically (every 60 seconds by default)
3. Maximum TTL = 32 hops (rather than the 16 hops in RIP)
4. Mask included in route update packet, CIDR supported.

Comparing to unicast routing, the multicast routing is a reversed route (i.e., you interested in where the packet comes from instead of where it is going to). That's why the route table information in DVMRP is used to determine whether the incoming multicast packet is arriving at the correct interface. The packet is discarded if the interface is not correct to prevent multicast loop.

The test to determine whether a packet is arriving at the correct interface is called RPF check. When a multicast packet arrives at an interface, the DVMRP route table will be checked to decide the reverse path to the source network. If the interface at which the packet arrives is the interface to send unicast information to the source, then the RPF check is success and the packet is forwarded from all down stream interfaces. Otherwise, there may be something wrong, and the multicast packet is discarded.

Since not all switches support multicast, DVMRP provide support for tunneling multicast information. Tunneling is a method used between DVMRP switches separated by non-multicast routing switch(es). The tunnel acts as the virtual network between two DVMRP switches. The multcast packet is encapsulated in a unicast packet and destined to a multicast-enabled switch. DVMRP treats tunneling interface the same way as common physical interfaces.

If two or more switches are connected to a multi-egress network, multiple copies of a packet may be sent to the subnet. Therefore, a specific forwarder must be specified. DVMRP fulfills this by routing switch mechanism. When two switches in a multi-egress network are exchanging routing information, they know the route metric for each other to get to the source network, and the switch has the smallest metric to the source network becomes the designated forwarder of that subnet; if the metrics are same, the one with lower IP address rules.

When DVMRP is enabled on an interface of the switch, probe messages are multicasted to the other DVMRP switches to discover the neighbors and their capabilities. If no probe message from a neighbor is received before the neighbor timeout, it is regarded as lost.

In DVMRP, source network route selection information is exchanged in the same basic

way like the RIP. That is to say, route advertisements are sent between DVMRP neighbors periodically (every 60 seconds by default). The routing information in the DVMRP route selection table is used to establish the source distribution tree, which can be used to determine which neighbor can reach the source sending multicast information. Interfaces leading to this neighbor are referred to as the upstream interface. Routing report packet contains source network and the hops for assessing route metrics.

To forward properly, each DVMRP switch need to know in what specific interface the multicast information should be received for the downstream switches. When a multicast packet from a specific source is received, a DVMRP switch will first broadcast the multicast packet in all downstream interfaces (interfaces in which other DVMRP switches have indicated dependency). On receiving a prune message from a downstream switch, that switch will be pruned. The DVMRP switch informs a upstream switch for a certain source by poison reverse: “I am your downstream.” The DVMRP switch fulfills the poison reverse by adding infinite (32) to the route metric of a certain source broadcasted by it in replying its upstream switches. Hence correct metric value can be 1 to (2 x infinite (32) -1), or 1 to 63. 1 to 31 indicates a reachable source network, 32 indicates an unreachable source, 33 to 63 indicate the switch generating the report message depend on upstream switches to receive multicast information from certain source.

16.5.2 DVMRP configuration

16.5.2.1 Configuration Task Sequence

1. Enable DVMRP (required)
2. Configure connectivity with CISCO routers/switches (optional)
3. Configure DVMRP sub-parameters (optional)

(1) Configuring DVMRP interface parameters.

a. Configure metric value for DVMRP report packet

b. Configuring DVMRP neighbor timeout time

(2) Configuring DVMRP global parameters.

a. Configure retransmission interval for graft packets in DVMRP

b. Configure transmission interval of probe packets in DVMRP

c. Configure transmission interval of report packets in DVMRP

d. Configuring DVMRP route timeout time

4. Configure DVMRP tunneling
5. Disable DVMRP

1. Enable DVMRP

Basic configuration of DVMRP routing protocol on route switch is quite simple: just enable DVMRP in the appropriate interfaces.

Command	Explanation
Interface Mode	

[no] ip dvmrp	Enable DVMRP; the "**no ip dvmrp enable**" command disables DVMRP (required)

2. Configure connectivity with CISCO routers/switches

CISCO does not really implemented DVMRP, but provides connectivity with DVMRP. As CISCO routers/switches send report packet but not probe packets, neighbor timeout issue should be addressed in establish connectivity with CISCO routers/switches. The following command makes a DSRS-5950 switch to decide the timeout of a neighbor by report packet intervals.

Command	Explanation
Interface Mode	
[no] ip dvmrp cisco-compatible <*A.B.C.D*>	Enable connectivity with CISCO neighbor A, B, C, D; the "**no ip dvmrp cisco-compatible**" command disables connectivity with CISCO neighbors.

3. Configure DVMRP sub-parameters

(1) Configuring DVMRP interface parameters.

a. Configure metric value for DVMRP report packet

b. Configuring DVMRP neighbor timeout time

Command	Explanation
Interface Mode	
ip dvmrp metric <*metric_val*> **no ip dvmrp metric**	Set interval for sending DVMRP report packets in the interface; the "**no ip dvmrp metric**" command restores the default setting.
ip dvmrp nbr-timeout <*time_val* > **no ip dvmrp nbr-timeout**	Set timeout interval for DVMRP neighbors in the interface; the "**no ip dvmrp nbr-timeout**" command restores the default setting.

(2) Configuring DVMRP global parameters.

a. Configure transmission interval of graft packets in DVMRP

b. Configure transmission interval of probe packets in DVMRP

c. Configure transmission interval of report packets in DVMRP

Command	Explanation
Global Mode	
ip dvmrp graft-interval <*time_val*> **no ip dvmrp graft-interval**	Set the interval for sending DVMRP graft messages; the "**no ip dvmrp graft-interval**" command restores the default setting.
ip dvmrp probe-interval <*time_val*> **no ip dvmrp probe -interval**	Set the interval for sending DVMRP probe messages; the "**no ip dvmrp probe interval**" command restores the default setting.

ip dvmrp report-interval <*time_val*> **no ip dvmrp report-interval**	Set the interval for sending DVMRP report messages; the "**no ip dvmrp report interval**" command restores the default setting.

d. Configuring DVMRP route timeout time

Command	Explanation
Global Mode	
ip dvmrp route-timeout <*time_val*> **no ip dvmrp route-timeout**	Set timeout interval for DVMRP routes; the "**no ip dvmrp route-timeout**" command restores the default setting.

4. Configure DVMRP tunneling

Command	Explanation
Interface Mode	
ip dvmrp tunnel <*A.B.C.D*> [metric <*metric_val*>] **no ip dvmrp tunnel <*A.B.C.D*>**	Configure tunneling to neighbor A, B, C, D; the "**no ip dvmrp tunnel**" command removes the tunnel to neighbor A, B, C, D.

5. Disable DVMRP

Command	Explanation
Interface Mode	
no ip dvmrp enable	Disable DVMRP

16.5.2.2 DVMRP Configuration Commands

- **ip dvmrp cisco-compatible**
- **ip dvmrp**
- **ip dvmrp graft-interval**
- **ip dvmrp metric**
- **ip dvmrp nbr-timeout**
- **ip dvmrp probe-interval**
- **ip dvmrp report-interval**
- **ip dvmrp route-timeout**
- **ip dvmrp tunnel**
- **show ip dvmrp mroute**
- **show ip dvmrp neighbor**
- **show ip dvmrp route**
- **show ip dvmrp tunnel**
- **debug ip dvmrp detail**
- **debug ip dvmrp pruning**

16.5.2.2.1 ip dvmrp cisco-compatible

Command: ip dvmrp cisco-compatible <*A.B.C.D*>
no ip dvmrp cisco-compatible <*A.B.C.D*>

Function: Enable connectivity with CISCO neighbor A, B, C, D; the "**no ip dvmrp cisco-compatible**" command disables connectivity with CISCO neighbors.

Parameter: <*A.B.C.D*> are the Neighboring IP addresses

Default: The connectivity with CISCO neighbors is disabled by default.

Command mode: Interface Mode

Usage Guide: CISCO does not really implemented DVMRP, but provides connectivity with DVMRP. As CISCO routers/switches send report packet but not probe packets, neighbor timeout issue should be addressed in establish connectivity with CISCO routers/switches. Configuration of this command enables the switch to tell neighbor timeout by report packet intervals (if no report message format a CISCO neighbor is received in an interval three times of the report interval, that neighbor is considered to be timeout.

Example: Enable connectivity with CISCO neighbor 1.1.1.1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp cisco-compatible 1.1.1.1

16.5.2.2.2 ip dvmrp

Command: ip dvmrp
no ip dvmrp

Function: Enable DVMRP on the interface; the "**no ip dvmrp enable**" command disables DVMRP on the interface.

Parameter: N/A.

Default: DVMRP is disabled by default.

Command mode: Interface Mode

Usage Guide:

Example: Enable DVMRP on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp

16.5.2.2.3 ip dvmrp graft-interval

Command: ip dvmrp graft-interval <*time_val*>
no ip dvmrp graft-interval

Function: Set the interval for sending DVMRP graft messages; the "**no ip dvmrp**

graft-interval" command restores the default setting.

Parameter: <***time_val***> is the interval for sending DVMRP graft packets, ranging from 5 to 3600s.

Parameter: The default interval for sending DVMRP graft messages is 5s.

Command mode: Global Mode

Usage Guide: If a new receiver joins that interface when an interface is in the pruned state, the interface will send a graft message to the upstream; if no graft ACK message from the upstream is received, it will keep sending graft message to the upstream at regular interval until an appropriate graft ACK is received.

Example: Set the interval for sending DVMRP graft messages to 10s.

Switch (Config)#ip dvmrp graft-interval 10

16.5.2.2.4 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>
no ip dvmrp metric

Function: Set interval for sending DVMRP report packets in the interface; the "**no ip dvmrp metric**" command restores the default setting.

Parameter: **< *metric_val*>** is the route metric value, ranging from 1 to 32.

Default: The default tag value is 1.

Command mode: Interface Mode

Usage Guide: The routing information in a DVMRP report packet includes a list of source network addresses and metrics. When DVMRP report packet metric is configured on the interface, all route entries received on that interface will be added the interface metric value configured to form a new metric value. The metric value is used for poison reverse calculation to determine upstream/downstream conditions. If a route metric in the local switch is greater than 32 or equal to 32, then this route is unreachable. If after calculation, the switch confirms itself in the downstream of a route, then a report message containing that route will be sent to the upstream, with the metric added by 32 to indicate the downstream position.

Example: Configure the DVMRP report packet metric to 2 on the interface.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp metric 2

16.5.2.2.5 ip dvmrp nbr-timeout

Command: ip dvmrp nbr-timeout <*time_val*>
no ip dvmrp nbr-timeout

Function: Set timeout interval for DVMRP neighbors in the interface; the "**no ip dvmrp nbr-timeout**" command restores the default setting.

Parameter: < *time_val*> is the time to timeout a neighbor, the valid range is 20 to 8000s.

Default: The default neighbor timeout setting is 35 seconds.

Command mode: Interface Mode

Usage Guide: When neighborhood established in DVMRP, a neighbor is considered nonsexist if no probe message from that neighbor is received in the neighbor timeout interval, and the neighborhood is terminated. Neighbor timeout interval must be greater than the interval for sending probe messages.

Example: Configure the DVMRP neighbor timeout interval for the interface to 30s.

Switch (Config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp nbr-timeout 30

16.5.2.2.6 ip dvmrp probe-interval

Command: ip dvmrp probe-interval <*time_val*>

no ip dvmrp probe-interval

Function: Set the interval for sending DVMRP probe messages; the "**no ip dvmrp probe interval**" command restores the default setting.

Parameter: <***time_val***> is the interval for sending DVMRP probe packets, ranging from 5 to 30s.

Default: The default interval for sending DVMRP probe messages is 10s.

Command mode: Global Mode

Usage Guide: The probe message enables DVMRP switches to locate each other and establish the neighborhood, and to learn the capability of each other. DVMRP switches claim their existence by sending probe message to their neighbors. If no probe message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time must be no greater than the neighbor timeout time.

Example: Set the interval for sending DVMRP probe messages to 20s.

Switch (Config)#ip dvmrp probe-interval 20

16.5.2.2.7 ip dvmrp report-interval

Command: ip dvmrp report-interval <*time_val*>

no ip dvmrp report-interval

Function: Set the interval for sending DVMRP report messages; the "**no ip dvmrp report-interval**" command restores the default setting.

Parameter: <***time_val***> is the interval for sending DVMRP report packets, ranging from 10 to 2000s.

Default: The default interval for sending DVMRP report messages is 60s.

Command mode: Global Mode

Usage Guide: DVMRP route information is exchanged in the way similar to that in RIP, i.e., in the report messages between DVMRP neighbors periodically. If no

updating report message for a route from the neighbor of the route is received in the specified interval, then the route is considered to be invalid. This interval configured must be no greater than the timeout interval for the route.

Example: Set the interval for sending DVMRP route report messages to 100s.

Switch (Config)#ip dvmrp report-interval 100

16.5.2.2.8 ip dvmrp route-timeout

Command: ip dvmrp route-timeout <time_val>

no ip dvmrp route-timeout

Function: Set timeout interval for a DVMRP route; the "**no ip dvmrp route-timeout**" command restores the default setting.

Parameter: < *time_val*> is the time to timeout a route, the valid range is 20 to 1400s.

Default: The default timeout setting for DVMRP routes is 140 seconds.

Command mode: Global Mode

Usage Guide: If no updating report message for a route from the neighbor of the route is received in the specified interval, then the route is considered to be invalid. This timeout interval must be greater than that for sending report messages.

Example: Configure the DVMRP route timeout interval to 100s.

Switch (Config)#ip dvmrp route-timeout 100

16.5.2.2.9 ip dvmrp tunnel

Command: ip dvmrp tunnel <*A.B.C.D*> [metric <*metric_val*>]

no ip dvmrp tunnel <*A.B.C.D*>

Function: Configure tunneling to neighbor A, B, C, D; the "**no ip dvmrp tunnel**" command removes the tunnel to neighbor A, B, C, D.

Parameter: < *A.B.C.D*> is the IP addresses of remote neighbors; **<*metric_val*>** is the metric value for the tunnelling interface, ranging from 1 to 32.

Default: DVMRP tunneling is disabled by default, the default value for **<*metric_val*>** is 1.

Command mode: Interface Mode

Usage Guide: Since not all switches support multicast, DVMRP provide support for tunneling multicast information. Tunneling is a method used between DVMRP switches separated by non-multicast routing switch(es). The tunnel acts as the virtual network between two DVMRP switches. The multicast packet is encapsulated in a unicast packet and destined to a

multicast-enabled switch. DVMRP treats tunneling interface the same way as common physical interfaces.

Example: Configure a DVMRP tunnel on Ethernet interface vlan1 to the remote neighbor 1.1.1.1.

Switch(Config-If-Vlan1)#ip dvmrp tunnel 1.1.1.1 metric 10

16.5.3 Typical DVMRP Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and DVMRP protocol is enabled on each vlan interface.

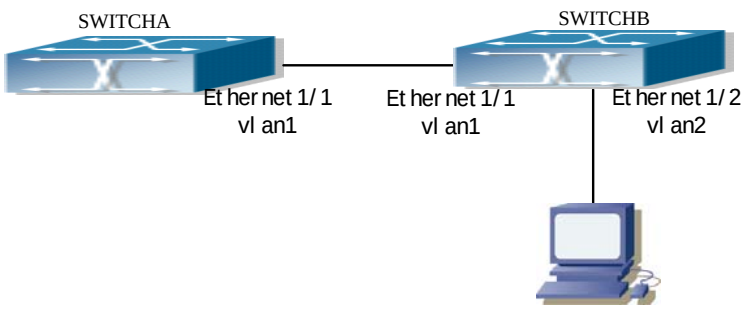


Fig 16-3 DVMRP network topology

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SWITCHA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp

(2) Configuration of SWITCHB:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan2)# ip dvmrp

16.5.4 DVMRP Troubleshooting Help

1. Monitor and debug commands
2. DVMRP troubleshooting help

16.5.4.1 Monitor and Debug Commands

16.5.4.1.1 show ip dvmrp mroute

Command: show ip dvmrp mroute

Function: Display the DVMRP packet forwarding entries..

Parameter: N/A.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: This command is used to display DVMRP multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example:

Switch# show ip dvmrp mroute

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

DVMRP Multicast Routing Table, inodes 1 routes 1:

(192.168.1.0, 224.1.1.1), protos: 0x2, flags: 0x0
Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 1
Outgoing interface list:
(Vlan2), protos: 0x2
Upstream prune interface list:
Downstream prune interface list:

Displayed information	Explanation
(192.168.1.0, 224.1.1.1)	Forwarding entry.
Incoming interface	Incoming interface, or RPF interface.
Outgoing interface list	Outgoing interface list.
Upstream prune interface list	Upstream prune interface list.
Downstream prune interface list	Downstream prune interface list.

16.5.4.1.2 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [<*ifname*>]

Function: Display information for DVMRP neighbors.

Parameter: ***<ifname>*** is the interface name, i.e. display neighbor information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Display neighbor information of Ethernet interface vlan1.

Switch #show ip dvmrp neighbor vlan1

Switch #

Neighbor-Address	Interface	Uptime	Expires
192.168.1.22	Vlan1	00: 02: 22	00: 00: 28

Switch #

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The interface on which the neighbor is discovered.
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.

16.5.4.1.3 show ip dvmrp route

Command: show ip dvmrp route

Function: Display DVMRP routing information.

Parameter: N/A.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: This command is used to display DVMRP route table entries; DVMRP maintains separated unicast route table for RPF check.

Example: Display DVMRP routing information.

Switch #show ip dvmrp route

Switch #

Destination/Mask	Nexthop	Interface	Gateway	Metric	state
192.168.1.0/24	192.168.1.11	Vlan1	No-Gateway	1	active

Switch #

Displayed information	Explanation
Destination/Mask	Target network segment or address and

	mask.
Nexthop	Next hop address
Interface	The interface on which the route is discovered.
Gateway	Gateway address
Metric	Route metric value
state	Route state (active, hold, etc)

16.5.4.1.4 show ip dvmrp tunnel

Command: show ip dvmrp tunnel [<*ifname*>]

Function: Display information for a DVMRP tunnel.

Parameter: ***<ifname>*** is the interface name, i.e. display the tunnel information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Display tunneling configuration information of Ethernet interface vlan1.

Switch #show ip dvmrp tunnel vlan1

Name: dvmrp2, Index: 7, State: 1195, Parent: 3, Localaddr: 192.168.1.11, Remote: 1.1.1.1

Switch #

Displayed information	Explanation
Name	Tunnel interface name (auto-generated by the system)
Index	Tunnel interface index number
State	Tunnel interface status
Parent	The index number of the parent interface for the tunnel interface
Localaddr	Local address of the tunnel interface
Remote	Remote end address of the tunnel

16.5.4.1.5 debug ip dvmrp detail

Command: debug ip dvmrp detail

Function: Enable the debug function for displaying detailed DVMRP information; the "**no**" format of this command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about DVMRP packets (except prune and graft) is required, this debug command can be used.

Example:

Switch#debug ip dvmrp detail
DVMRP detail debug is on
Switch#01: 18: 09: 35: DVMRP: Received probe on vlan1 from 192.168.1.22
01: 18: 09: 35: DVMRP: probe Vers: majorv 3, minorv 255
01: 18: 09: 35: DVMRP: probe flags: PG
01: 18: 09: 35: DVMRP: probe genid: 0x48
01: 18: 09: 35: DVMRP: probe nbrs: 192.168.1.11
01: 18: 09: 40: DVMRP: Send probe on vlan1 to 224.0.0.4, len 16
01: 18: 09: 40: DVMRP: probe Vers: majorv 3, minorv 255
01: 18: 09: 40: DVMRP: probe flags: PG
01: 18: 09: 40: DVMRP: probe genid: 0x24c57
01: 18: 09: 40: DVMRP: probe nbrs: 192.168.1.22
01: 18: 09: 40: DVMRP: Send probe on dvmrp2 to 224.0.0.4, len 12
01: 18: 09: 40: DVMRP: probe Vers: majorv 3, minorv 255
01: 18: 09: 40: DVMRP: probe flags: PG
01: 18: 09: 40: DVMRP: probe genid: 0x24f29

16.5.4.1.6 debug ip dvmrp pruning

Command: debug ip dvmrp pruning
no debug ip dvmrp pruning

Function: Enable the debug function for displaying DVMRP prune/graft information; the "**debug ip dvmrp pruning**" command disables this debug function.

Parameter: N/A.

Default: Debug is disabled by default.

Command mode: Admin Mode

Usage Guide: If detailed DVMRP prune/graft information is required, this debug command can be used.

Example:

Switch#debug ip dvmrp pruning
DVMRP pruning debug is on
02: 22: 20: 26: DVMRP: Received prune on vlan2 from 105.1.1.2, len 20
02: 22: 20: 26: DVMRP: Prune Vers: majorv 3, minorv 255
02: 22: 20: 26: DVMRP: Prune source 192.168.1.105, group 224.1.1.1
02: 22: 20: 40: DVMRP: Received graft on vlan1 from 105.1.1.2, len 16
02: 22: 20: 40: DVMRP: Graft Vers: majorv 3, minorv 255

02: 22: 20: 40: DVMRP: Graft source 192.168.1.105, group 224.1.1.1

02: 22: 20: 40: DVMRP: Send graft-ACK on vlan1 to 105.1.1.2, len 16

02: 22: 20: 40: DVMRP: Graft-Ack Vers: majorv 3, minorv 255

02: 22: 20: 40: DVMRP: Graft-ACK source 192.168.1.105, group 224.1.1.1

16.5.4.2 DVMRP Troubleshooting Help

In configuring and using DVMRP protocol, the DVMRP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interfaces status” command).
- ✧ Ensure the interface has an IP address properly configured (use “ip address” command).
- ✧ Next, enable DVMRP on the interface (use the “ip dvmrp” command).
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured. (DVMRP uses its own unicast route table, use the “show ip dvmrp route” command to view that table.)
- ✧ If connectivity with CISCO is required, make sure the CISCO connex command is configured (use “ip dvmrp cisco-compatible” command)

16.6 IGMP

16.6.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is a TCP/IP protocol responsible for IP multicast member management. It is used to establish and maintain multicast group membership between IP hosts and direct neighbor multicast switches. IGMP does not include the populating and maintenance of membership between multicast switches, which is covered by multicast routing protocols. All hosts participate in multicast must implement IGMP.

Hosts participate in IP multicast can join/quit multicast groups at any position, any time, and of any number. The multicast switches do not save all host memberships, which is also impractical. They just obtain information about whether receivers of a multicast group (group member) exist in network segments connecting to its interfaces. As to the hosts, they only need to keep the information about the multicast groups joined.

IGMP is asymmetric for hosts and switches: The hosts respond IGMP query packets sent

by the multicast switches, i.e., respond with membership report packets. The switches send membership query packets in regular interval, and decide whether hosts of their subnet join some group or not; on receiving quit group reports from the hosts, they send query of associated group (IGMP v2) to determine whether there are members in a certain group.

There are so far three versions of IGMP: IGMP v1 (define in RFC1112), IGMP v2 (defined in RFC2236) and IGMP v3. Version 2 is the most widely used version at present.

Major improvements of IGMP v2 from v1 include:

1. Election mechanism for multicast switches in shared network segments.

A share network segment is a segment with several multicast switches. In this case, since all switches running IGMP in the segment can receive membership report messages, only one switch is needed to send membership query message. Therefore, there should be a switch election mechanism to determine the switch acting as the querier. In IGMP v1, the selection of querier is determined by multicast routing protocols; IGMP v2 improves this feature and specifies the multicast switch of the lowest IP address to be the querier.

2. Quit group mechanism added in IGMP v2

In IGMP v1, the hosts quit the multicast without giving any message to any multicast switch. And multicast switches have to decide the quit of multicast member by multicast group response timeout. In version2, if a host decides to quit a multicast group, and it is the host responding to the latest membership query message, it sends a quit-group message.

3. Specific group query added in IGMP v2

In IGMP v1, the query of multicast switch aims for all multicast groups in that segment. This query is called the universal group query. In IGMP v2, specific group query is introduced in addition to the universal group query. The destination IP address of such query packet is the IP address of the specified multicast group, the area part in the packet of the group address is the IP address of the specified multicast group, too. Thus response packets from the hosts of the other multicast groups can be avoided.

4. Maximum response time field added in IGMP v2

IGMP v2 has a field for maximum response time added,, so that hosts response time for group query packets can be adjusted dynamically.

16.6.2 IGMP configuration

16.6.2.1 Configuration Task Sequence

1、 Enable IGMP (required)

Configure IGMP sub-parameters (optional)

(1) Configure IGMP group parameters.

a. Configuring IGMP group filtering criteria

b. Configure IGMP groups

c. Configure static IGMP groups

(2) Configure IGMP query parameters.

a. Configure transmission interval of query packets in IGMP

b. Configure maximum response time for IGMP queries

c. Configure timeout setting for IGMP queries

(3) Configure IGMP version

2、 Disable IGMP

1. Enable IGMP

There is no special command for enabling IGMP in layer3 switches, the IGMP automatically enables when any multicast protocol is enabled on the respective interface.

Command	Explanation
Interface Mode	
ip dvmrp | ip pim dense-mode | ip pim sparse-mode	Enable IGMP protocol; the "**no pim sparse-mode**" command disables IGMP protocol (required)

2. Configure IGMP sub-parameters

(1) Configure IGMP group parameters.

a. Configuring IGMP group filtering criteria

b. Configure IGMP groups

c. Configure static IGMP groups

Command	Explanation
Interface Mode	
ip igmp access-group {<*acl_num* | *acl_name*>} **no ip igmp access-group**	Set the filter criteria for IGMP group on the interface; the "**no ip igmp access-group**" command cancels the filter criteria.
ip igmp join-group <*A.B.C.D* > **no ip igmp join-group <*A.B.C.D* >**	Join the interface to an IGMP group; the "**no ip igmp join-group**" command cancels the join.
ip igmp static-group <*A.B.C.D* > **no ip igmp static -group <*A.B.C.D* >**	Join the interface to a static IGMP group; the "**no ip igmp static -group**" command cancels the join.

(2) Configure IGMP query parameters.

a. Configure transmission interval of query packets in IGMP

b. Configure maximum response time for IGMP queries

c. Configure timeout setting for IGMP queries

Command	Explanation

Interface Mode	
ip igmp query-interval <*time_val*> **no ip igmp query-interval**	Set the interval for sending IGMP query messages; the "**no ip IGMP query interval**" command restores the default setting.
ip igmp query-max-response-time <*time_val*> **no ip igmp query-max-response-time**	Set the maximum time for a interface to response to a IGMP query; the "**no ip igmp query-max-response-time**" command restores the default setting.
ip igmrp query-timeout <*time_val*> **no ip igmp query-timeout**	Set the timeout interval for a interface to response to a IGMP query; the "**no ip igmp query-timeout**" command restores the default setting.

(3) Configure IGMP version

Command	Explanation
Interface Mode	
ip igmp version <*version*> **no ip igmp version**	Configure the IGMP version of the interface; the "**no ip igmp version**" command restores the default setting.

3. Disable IGMP

Command	Explanation
Interface Mode	
no ip dvmrp | no ip pim dense-mode | no ip pim sparse-mode	Disable IGMP

16.6.2.2 IGMP Configuration Commands

- **ip igmp access-group**
- **ip igmp join-group**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp query-timeout**
- **ip igmp static-group**
- **ip igmp version**
- **show ip igmp groups**
- **show ip igmp interface**
- **debug ip igmp event**
- **debug ip igmp packet**

16.6.2.2.1 ip igmp access-group

Command: ip igmp access-group {<*acl_num* | *acl_name*>}
no ip igmp access-group

Function: Set the filter criteria for IGMP group on the interface; the "**no ip igmp access-group**" command cancels the filter criteria.

Parameter: {<*acl_num* | *acl_name*>} is the sequence number of name of the access list, where the range of ***acl_num*** is 1 to 99.

Default: No filter criteria set by default

Command mode: Interface Mode

Usage Guide: This command can be sued to filter the groups on the interface to allow or deny the participant of some groups.

Example: Specify interface vlan1 to permit 224.1.1.1 and deny 224.1.1.2.

Switch (Config)#access-list 1 permit 224.1.1.1 0.0.0.0
Switch (Config)#access-list 1 deny 224.1.1.2 0.0.0.0
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp access-group 1

16.6.2.2.2 ip igmp join-group

Command: ip igmp join-group <*A.B.C.D* >
no ip igmp join-group <*A.B.C.D* >

Function: Join the interface to an IGMP group; the "**no ip igmp join-group**" command cancels the join.

Parameter: <*A.B.C.D*> are the IP addresses for multicast groups.

Default: Do not join groups.

Command mode: Interface Mode

Usage Guide: When a switch is used as a host, this command is used to any the host to a group; Suppose the local interface is to be added to group 224.1.1.1, then the switch will send a IGMP member report containing group 224.1.1.1 on receiving IGMP group query from the other switches. Note the difference between this command and the "**ip igmp static-group**" command.

Example: Specify interface vlan1 to join group 224.1.1.1.

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

16.6.2.2.3 ip igmp query-interval

Command: ip igmp query-interval <*time_val*>
no ip igmp query-interval

Function: Set the interval for sending IGMP query messages; the "**no ip IGMP query interval**" command restores the default setting.

Parameter: <***time_val***> is the interval for sending IGMP query packets, ranging from 1 to 65535s.

Default: The default interval for sending IGMP query messages is 125s.

Command mode: Interface Mode

Usage Guide: When a multicast protocol enables on a interface, IGMP query message will be sent at regular interval from this interface. This command is also used to configure the query period.

Example: Set the interval for sending IGMP query messages to 10s.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-interval 10

16.6.2.2.4 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <*time_val*>
no ip igmp query- max-response-time

Function: Set the maximum time for a interface to response to a IGMP query; the "**no ip igmp query-max-response-time**" command restores the default setting.

Parameter: <***time_val***> is the maximum interface response time for IGMP queries, ranging from 1 to 25s.

Default: The default value is 10 seconds.

Command mode: Interface Mode

Usage Guide: On receiving a query message from the switch, the host will set a counter for each multicast group it belongs to, the counter value is random from 0 to the maximum response time. When the value of any counter decreases to 0, the host will send the member report message for the multicast group. Set the maximum response time sensibly enable fast responds of host to query messages, the router can also get the existing status of the multicast group members.

Example: Set the maximum IGMP query response time to 20 seconds.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query- max-response-time 20

16.6.2.2.5 ip igmp query-timeout

Command: ip igmp query-timeout <*time_val*>
no ip igmp query-timeout

Function: Set the timeout interval for a interface to response to a IGMP query; the "**no ip igmp query-timeout**" command restores the default setting.

Parameter: < *time_val*> is the time to timeout a IGMP query, the valid range is 60 to

300s.

Default: The default value is 265 seconds.

Command mode: Interface Mode

Usage Guide: In a shared network with several routers running IGMP, one switch will be selected as the querier for that shared network, the other switches act as timers monitoring the status of the querier; if no query packet from the querier is received after the query timeout time, a new switch will be elected to be the new querier.

Example: Configure the interface timeout setting for IGMP queries to 100s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-timeout 100

16.6.2.2.6 ip igmp static-group

Command: ip igmp static-group <*A.B.C.D* >

no ip igmp static -group <*A.B.C.D* >

Function: Join the interface to an IGMP static group; the "**no ip igmp static -group**" command cancels the join.

Parameter: <*A.B.C.D*> are the IP addresses for multicast groups.

Default: Do not join static groups.

Command mode: Interface Mode

Usage Guide: After an interface joins a static group, then the interface will receive multicast packet about that static group regardless of whether there are actual receivers under the interface or not; for instance, if the local interface joins static group 224.1.1.1., then the local interface will keep receiving multicast packets about he group 224.1.1.1 regardless of whether there are receiver of not under the interface. Note the difference between this command and the "**ip igmp join-group**" command.

Example: Specify interface vlan1 to join static group 224.1.1.1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1

16.6.2.2.7 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configure the IGMP version of the interface; the "**no ip igmp version**" command restores the default setting.

Parameter: <*version*> is the IGMP version configured, v1 and v2 are supported at present.

Default: The default version number is v2.

Command mode: Interface Mode

Usage Guide: This command is used to provide forward compatibility between different versions. It should be noted that v1 and v2 are not interconnectable, and the same version of IGMP must be ensured for the same network.

Example: Configure the IGMP running on the interface to version 1.

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp version 1
```

16.6.3 Typical IGMP Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and PIM-DM protocol is enabled on each vlan interface.

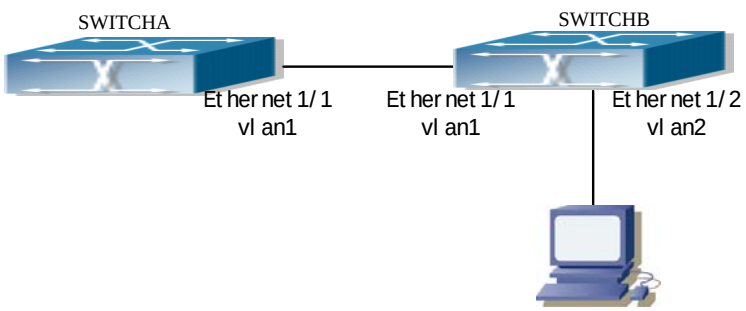


Fig 16-4 IGMP network topology

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SWITCHA:

```
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim dense-mode
```

(2) Configuration of SWITCHB:

```
Switch(Config)#interface vlan1
Switch(Config-If-Vlan1)#ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch(Config)#interface vlan2
Switch(Config-If-Vlan2)#ip pim dense-mode
Switch(Config-If-Vlan2)#ip igmp version 1
Switch(Config-If-Vlan2)#ip igmp query-timeout 150
```

16.6.4 IGMP Troubleshooting Help

1. Monitor and debug commands

2.IGMP Troubleshooting Help

16.6.4.1 Monitor and Debug Commands

16.6.4.1.1 show ip igmp groups

Command: show ip igmp groups [{<*ifname* | *group_addr*>}]

Function: Display IGMP group information.

Parameter: <*ifname*> is the interface name, i.e. display group information of the specified interface; **<*group_addr*>** is the group address, i.e., view group information.

Default: Not displayed.

Command mode: Admin Mode

Example:

Switch#show ip igmp groups

IGMP Connect Group Membership (1 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
239.255.255.250	Vlan123	02: 57: 30	00: 03: 36	123.1.1.2

Switch#

Displayed information	Explanation
Group Address	Multicast group IP address
Interface	Interface of the multicast group
Uptime	The up time of the multicast group
Expires	Rest time before the multicast group timeouts
Last Reporter	The host last reported the multicast group

16.6.4.1.2 show ip igmp interface

Command: show ip igmp interface [<*ifname*>]

Function: Display IGMP related information on the interface

Parameter: <*ifname*> is the interface name, i.e. display IGMP information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Display IGMP information of Ethernet interface vlan1.

Switch # show ip igmp interface vlan1

Vlan1 is up, line protocol is up

Internet address is 192.168.1.11, subnet mask is 255.255.255.0

IGMP is enabled, I am querier

IGMP current version is V2

IGMP query interval is 125s

IGMP querier timeout is 265s

IGMP max query response time is 10s

Inboud IGMP access group is not set

Multicast routing is enable on interface

Multicast TTL threshold is 1

Multicast designed router (DR) is 192.168.1.22

Muticast groups joined by this system: 0

16.6.4.1.3 debug ip igmp event

Command: debug ip igmp event

Function: Enable the debug function for displaying IGMP events: the "**no**" format of this command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about IGMP events is required, this debug command can be used.

Example:

Switch# debug ip igmp event
igmp event debug is on

Switch# 01: 04: 30: 56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

16.6.4.1.4 debug ip igmp packet

Command: debug ip igmp packet

Function: Enable the IGMP packet debug function; the "**no debug ip ospf packet**" command disables this debug function.

Parameter: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If information about IGMP packets is required, this debug command can be

used.

Example:

Switch# debug ip igmp packet
igmp packet debug is on

Switch #02: 17: 38: 58: IGMP: Send membership query on dvmrp2 for 0.0.0.0

02: 17: 38: 58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0

02: 17: 39: 26: IGMP: Send membership query on vlan1 for 0.0.0.0

02: 17: 39: 26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0

16.6.4.2 IGMP Troubleshooting Help

In configuring and using IGMP protocol, the IGMP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interfaces status” command).
- ✧ Ensure at least one multicast protocol is enabled on the interface.
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured.

16.7 web Management

Click Multicast protocol configuration on the main page. Users can configure multicast protocols:

Multicast common configuration

PIM-DM configuration

PIM-SM configuration

DVMRP configuration

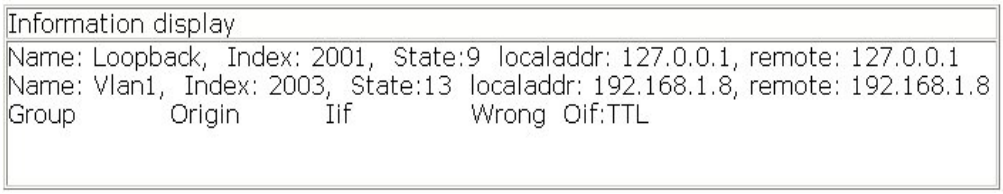
IGMP configuration

Inspect and debug

16.7.1 Multicast common configuration

In Multicast common configuration mode, click Show ip mroute to show ip multicast

packets forwarding. See the equivalent CLI command at 16.2.1.1.1. Users don't need to configure the parameters. For the detailed explanation of the displayed information, see chapter 16.2.1.1.1


Information display
Name: Loopback, Index: 2001, State:9 localaddr: 127.0.0.1, remote: 127.0.0.1
Name: Vlan1, Index: 2003, State:13 localaddr: 192.168.1.8, remote: 192.168.1.8
Group Origin Iif Wrong Oif:TTL

16.7.2 PIM-DM configuration

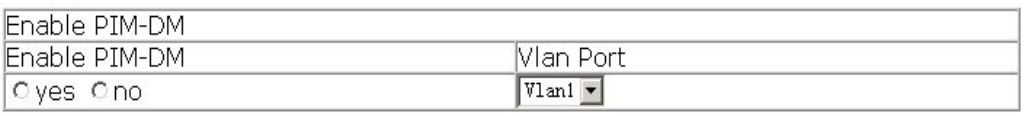
In PIM-DM configuration mode, users can enable PIM-DM or disable PIM-DM protocol on the port. See the equivalent CLI command at 16.3.2.3:

Enable PIM-DM – "yes" is used to enable PIM-DM protocol; "no" is used to disable PIM-DM protocol.

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Disable PIM-DM on the layer 3 interface



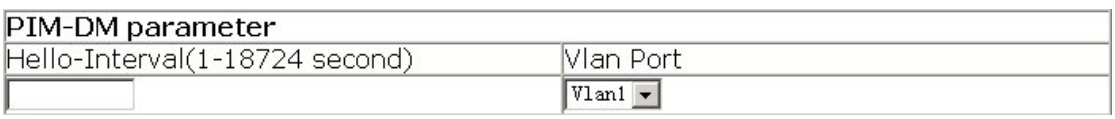
Click PIM-DM parameter configuration. Users can configure PIM-DM parameters on the layer 3 port. See the equivalent CLI command at 16.3.2.4:

Hello-Interval – Specify PIM-DM hello interval on the port

Vlan Port – Specify layer 3 vlan port

Apply – Apply the configuration

Default – Restore the default PIM-DM hello interval on the port



16.7.3 PIM-SM configuration

In PIM-SM configuration mode, users can enable PIM-SM or disable PIM-SM protocol on the port. See the equivalent CLI command at 16.4.2.2.1:

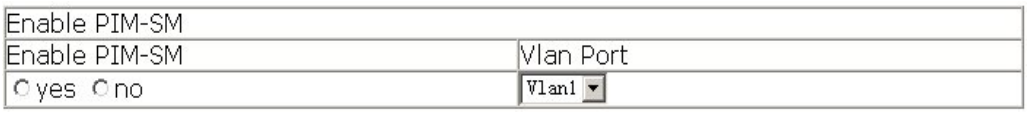
Enable PIM-SM – "yes" is used to enable PIM-SM protocol; "no" is used to disable

PIM-SM protocol.

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Disable PIM-SM on the layer 3 interface



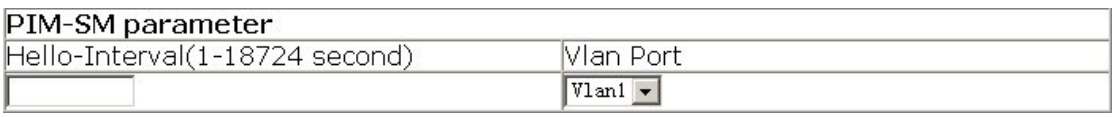
Click PIM-SM parameter configuration. Users can configure PIM-SM parameters on the layer 3 port. See the equivalent CLI command at 16.4.2.2.3:

Hello-Interval – Specify PIM-SM hello interval on the port

Vlan Port – Specify layer 3 vlan port

Apply – Apply the configuration

Default – Restore the default PIM-SM hello interval on the port

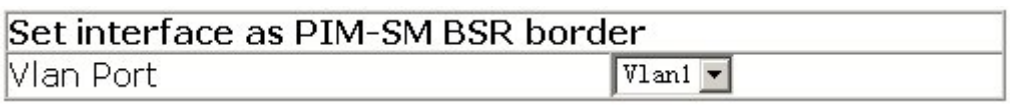


Click Set interface as PIM-SM BSR border. Users can configure the border port of PIM-SM area which can prevent BSR messages from advertising outside the PIM-SM area. See the equivalent CLI command at 16.4.2.2.2:

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Disable the port as PIM-SM area border



Click Set router as BSR candidate. Users can configure candidate BSR for PIM-SM. See the equivalent CLI command at 16.4.2.2.4:

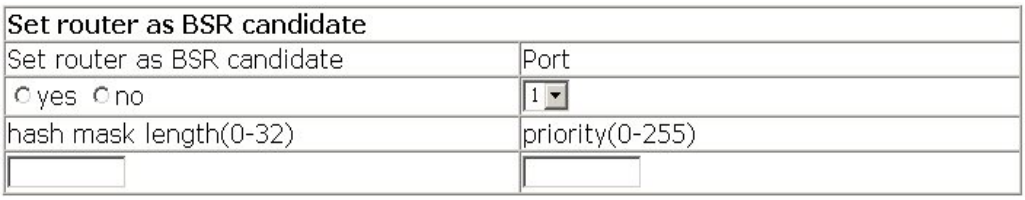
Set router as BSR candidate – “yes” is used to enable the switch as candidate BSR for PIM-SM; “no” is used to disable the switch as candidate BSR for PIM-SM

Port – Specify layer 3 VLAN ID

Hash mask length – Specify hash mask length

Priority – Specify priority

Apply – Apply the configuration



Click Set router as RP candidate. Users can configure candidate RP for PIM-SM. See the equivalent CLI command at 16.4.2.2.5:

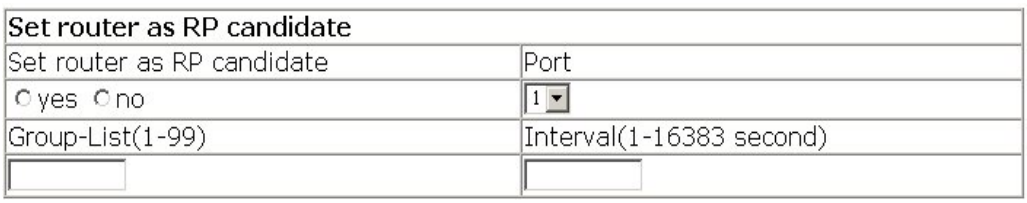
Set router as RP candidate – “yes” is used to set the switch as RP candidate; “yes” is used to cancel the switch as RP candidate

Port – Specify layer 3 VLAN ID

Group-List – Specify access-list number

Interval – Specify interval of sending candidate RP messages

Apply – Apply the configuration



16.7.4 DVMRP configuration

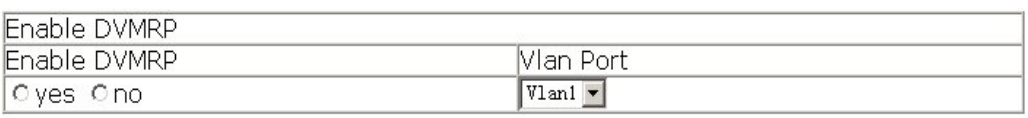
In DVMRP configuration mode, users can enable DVMRP or disable DVMRP protocol on the port. See the equivalent CLI command at 16.5.2.2.2:

Enable DVMRP – “yes” is used to enable DVMRP protocol; “no” is used to disable DVMRP protocol

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Disable DVMRP protocol



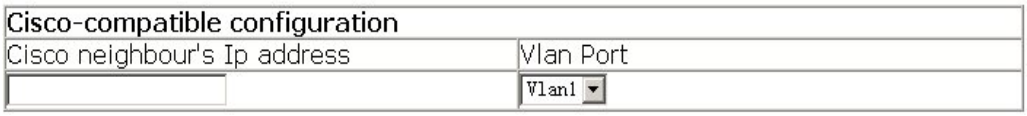
Click Cisco-compatible configuration. Users can enable Cisco-compatible. See the equivalent CLI command at 16.5.2.2.1:

Cisco neighbor’s IP address – Specify Cisco neighbor’s IP address

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Disable Cisco-compatible



Click DVMRP parameter configuration. Users can configure DVMRP interface parameters: See the equivalent CLI command at 16.5.2.2.4 and 16.5.2.2.5:

Vlan Port - Specify the layer 3 port

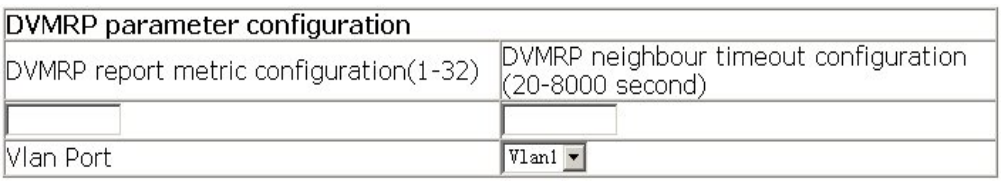
DVMRP report metric configuration – Configure DVMRP report metric for the port. See the equivalent CLI command at 16.5.2.2.4

DVMRP neighbor timeout configuration – Configure DVMRP neighbor timeout for the port. See the equivalent CLI command at 16.5.2.2.5

Apply – Apply the configuration

Default – Restore the default settings on the port (DVMRP report metric and DVMRP neighbor timeout)

Note: This page is related to two CLI commands. When users only set one parameter, there is a warning for not configuring the other parameter. The configuration is still valid.



Click DVMRP global parameter configuration. Users can configure global DVMRP parameters. See the equivalent CLI command at 16.5.2.2.3, 16.5.2.2.6, 16.5.2.2.7 and 16.5.2.2.8:

DVMRP graft interval configuration – Configure DVMRP graft interval. See the equivalent CLI command at 16.5.2.2.3

Interval of sending probe packet – Configure Interval of sending probe packet. See the equivalent CLI command at 16.5.2.2.6

Interval of sending report packet – Configure Interval of sending report packet. See the equivalent CLI command at 16.5.2.2.7

DVMRP route timeout – Configure DVMRP route timeout. See the equivalent CLI command at 16.5.2.2.8

Apply – Apply the configuration

Default – Restore the default settings (sending graft, probe, report interval, dvmrp route timeout)

Note: This page is related to four CLI commands. When users only set one parameter, there is a warning for not configuring other parameters. The configuration is still valid.

DVMRP global parameter configuration	
DVMRP graft interval configuration(5-3600 second)	Interval of sending probe packet(5-30 second)
Interval of sending report packet(10-2000 second)	DVMRP route timeout(20-1400 second)

Click DVMRP tunnel configuration. Users can create and delete DVMRP tunnel. See the equivalent CLI command at 16.5.2.2.9:

Neighbor ip address – Specify neighbor ip address

Metric – Specify metric to neighbor

Vlan Port –Specify the layer 3 port

Apply – Create DVMRP tunnel to neighbor

Delete tunnel - Delete DVMRP tunnel to neighbor

DVMRP tunnel configuration	
Neighbour ip address	Metric(1-32)
Vlan Port	Vlan1

16.7.5 IGMP configuration

In IGMP mode, click IGMP additive parameter configuration. Users can configure IGMP interface parameters. See the equivalent CLI command at 16.6.2.2.1, 16.6.2.2.2, 16.6.2.2.3, 16.6.2.2.4, 16.6.2.2.5 and 16.6.2.2.6:

Set Acl for IGMP group – Configure Acl for IGMP group. See the equivalent CLI command at 16.6.2.2.1

Add interface to IGMP group - Add interface to IGMP group. See the equivalent CLI command at 16.6.2.2.2

Add IGMP static group to VLAN - Add IGMP static group to VLAN. See the equivalent CLI command at 16.6.2.2.6

IGMP query interval – Configure IGMP query interval. See the equivalent CLI command at 16.6.2.2.3

Max-response IGMP request time – Configure Max-response IGMP request time. See the equivalent CLI command at 16.6.2.2.4

IGMP query timeout – Configure IGMP query timeout. See the equivalent CLI

command at 16.6.2.2.5

Vlan Port –Specify the layer 3 port

Apply – Apply the configuration

Default – Restore the default settings (including ACL for IGMP group, IGMP query interval, Max-response IGMP request time and IGMP query timeout. If users have configured static group and join group, the static group and the join group on the port are deleted.)

Note: This page is related to six CLI commands. When users only set one parameter, there is a warning for not configuring other parameters. The configuration is still valid.

IGMP additive parameter configuration	
Set ACL for IGMP group(1-99)	Add interface to IGMP group(A.B.C.D)
Add IGMP static group to VLAN(A.B.C.D)	IGMP query interval(1-65535 second)
Max-response IGMP request time(1-25 second)	IGMP query timeout(60-300 second)
Vlan Port	Vlan1

Click IGMP version configuration. Users can configure IGMP version. See the equivalent CLI command at 16.6.2.2.7:

IGMP version configuration – Specify IGMP version

Vlan Port - Specify the layer 3 port

Apply – Apply the configuration

Default – Restore the default IGMP version

IGMP version configuration	
IGMP version configuration(1 or 2)	
Vlan Port	Vlan1

16.7.6 Multicast inspect and debug

In Inspect and debug mode, click Show ip pim interface. The running PIM protocol interface information is shown. See the equivalent CLI command at 16.4.4.1.2

Click Show ip pim mroute dm. See the equivalent CLI command at 16.3.4.2

Click Show ip pim neighbor. See the equivalent CLI command at 16.3.4.3

Click Show ip pim bsr-router. See the equivalent CLI command at 16.4.4.1.1

Click Show ip pim mroute sm. See the equivalent CLI command at 16.4.4.1.3

Click Show ip pim rp. See the equivalent CLI command at 16.4.4.1.5

Click Show ip dvmrp mroute. See the equivalent CLI command at 16.5.4.1.1

Click Show ip dvmrp neighbor. See the equivalent CLI command at 16.5.4.1.2

Click Show ip dvmrp route. See the equivalent CLI command at 16.5.4.1.3

Click Show ip dvmrp tunnel. See the equivalent CLI command at 16.5.4.1.4

Chapter 17 VRRP Configuration

17.1 Introduction to VRRP

VRRP (Virtual Router Redundancy Protocol) is a redundancy protocol. It uses a backup mechanism to increase reliability of the router (or the layer 3 switch) to connect the outside network. It is designed for the local area network which supports multicast or broadcast, such as Ethernet. It is proposed by IETF, and widely used these days.

Normally, the default gateway should be configured on all the hosts in the LAN. When the hosts send packets whose destinations are not in the same subnet, these packets are sent to the default gateway. This configuration ensures the connection between the hosts in the subnet and the outside network. But when the connection between the default gateway and the outside network is down, all the hosts in the subnet can't communicate with the outside network.

The VRRP is developed to solve this problem. The VRRP is run on the multiple routers in the LAN. These routers form a virtual router and are called a standby group. In the standby group, there are one active router (called Master) and one or several backup routers (called Backup). The master router is responsible for forwarding the packets, whereas the backup routers serve as backups for the master router.

The virtual router has its virtual IP address which can be the same as the IP address of an interface of a router in the standby group. The backup routers also have their IP addresses. All the hosts in the LAN only need to set their default gateway to the virtual IP address of the virtual router, then they can communicate with the outside network. In fact, only the master router forwards the traffic. When the master router is down, one backup router takes it over, and the communication with the outside network is maintained.

Let's make a sum-up; In the VRRP standby group, there is always a master router which forwards the traffic; the other routers serve as backup routers. They monitor the status of the master router. When the master router is down, the backup routers select a new master router which forwards the traffic. This new election takes a very short time, so the hosts in the LAN can communicate with the outside work through the virtual router.

17.2 VRRP Configuration

17.2.1 VRRP Configuration Task Sequence

1. Create/Delete virtual router (required)
2. Configure VRRP virtual IP address and VRRP interface (required)
3. Enable/disable virtual router (required)
4. Configure VRRP authentication (optional)
5. Configure VRRP accessorial parameters (optional)
   （1）Configure VRRP preempt mode
   （2）Configure VRRP priority
   （3）Configure VRRP timer
   （4）Configure VRRP monitored interface

1. Create/Delete virtual router

Command	Explanation
Global Mode	
[no] router vrrp <*vrid*>	Create/Delete virtual router

2. Configure VRRP virtual IP address and interface

Command	Explanation
VRRP Mode	
virtual-ip <*ip*> {master| backup} **no virtual-ip**	Configure VRRP virtual IP address; the "**no virtual-ip**" command removes virtual IP address
interface{IFNAME | Vlan <*ID*>} **no interface**	Configure VRRP interface; the "**no interface**" command removes the interface

3. Enable/disable virtual router

Command	Explanation
VRRP Mode	
enable	Enable virtual router
disable	Disable virtual router

4. Configure VRRP authentication

Command	Explanation
Interface Mode	

ip vrrp authentication mode text **no ip vrrp authentication mode**	Configure authentication mode of VRRP messages sent by the current interface; the "**no ip vrrp authentication mode**" command restores the default authentication mode.
ip vrrp authentication string <*string*> **no ip vrrp authentication string**	Configure the authentication string of the VRRP packets sent on the interface; the "**no ip vrrp authentication string**" restores the default authentication string.

5. Configure VRRP accessorial parameters

（1）Configure VRRP preempt mode

Command	Explanation
VRRP Mode	
preempt-mode {true| false}	Configure VRRP preempt mode

（2）Configure VRRP priority

Command	Explanation
VRRP Mode	
priority < *priority* >	Configure VRRP priority

（3）Configure VRRP timer

Command	Explanation
VRRP Mode	
advertisement-interval <time>	Configure VRRP timer (in seconds)

（4）Configure VRRP monitored interface

Command	Explanation
VRRP Mode	
circuit-failover {IFNAME | Vlan <*ID*>} **no circuit-failover**	Configure the VRRP monitored interface; the "**no circuit-failover**" command deletes the monitored interface.

17.2.2 VRRP Configuration Commands

17.2.2.1 router vrrp

Command: router vrrp <*vrid*>

no router vrrp <*vrid*>

Function: Create/Delete virtual router

Parameter: < *vrid* > is the sequence number of the virtual router, valid range is 1 to 255.

Command mode: Global Mode

Usage Guide: This command is used to create or delete the virtual router. The virtual router is identified by the sequence numbers. Users have to create the virtual router before they configure the virtual router parameters.

Example: Configure the virtual router with sequence number 10.

Switch(config)# router vrrp 10

17.2.2.2 virtual-ip

Command: virtual-ip <*A.B.C.D*> {master| backup}

no virtual-ip

Function: Configure VRRP virtual IP address.

Parameter: <***A.B.C.D***> is virtual IP address in dotted decimal format.

Command mode: VRRP Mode

Usage Guide: This command is used to configure the virtual IP address for standby group; the “no virtual-ip” command deletes the virtual IP address for standby group. In one standby group, there is only one virtual IP address. The virtual IP address has two attributes: master and backup. If the virtual IP address is set to master, it has to be the same as the IP address of a router interface in the group. Accordingly, its VRRP priority is 255 (auto) and the relevant interface is the master router in the standby group; if the virtual IP address is set to backup, it can’t be the same as any IP address of the routers in the standby group. The virtual IP address and the interface IP addresses should be in the same subnet.

Example: Set backup virtual IP address to 10.1.1.1

Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1 backup

17.2.2.3 interface

Command: interface{IFNAME | Vlan <*ID*>}

no interface

Function: Configure the VRRP interface.

Parameter: interface{IFNAME | Vlan <*ID*>} is the interface name.

Command mode: VRRP Mode

Usage Guide: This command is used to add the layer 3 interface to the existing standby group; the “no interface” removes the layer 3 interfaces in the specified standby group.

Example: Configure the VRRP interface to interface vlan 1

Switch(Config-Router-Vrrp)# interface vlan 1

17.2.2.4 enable

Command: enable

Function: Enable the VRRP

Command mode: VRRP Mode

Usage Guide: Enable the virtual router. Users have to configure the VRRP virtual IP address and the VRRP interface before they enable the VRRP. After this configuration, the interface is added to the standby group.

Example: Enable the virtual router with the sequence number 10.

Switch(config)# router vrrp 10

Switch(Config-Router-Vrrp)# enable

17.2.2.5 disable

Command: disable

Function: Disable VRRP

Command mode: VRRP Mode

Usage Guide: Disable the relevant virtual router. Users have to disable VRRP before they change the VRRP configurations.

Example: Disable the virtual router with the sequence number 10.

Switch(config)# router vrrp 10

Switch (Config-Router-Vrrp)# disable

17.2.2.6 vrrp authentication mode

Command: ip vrrp authentication mode text

no ip vrrp authentication mode

Function: Set the authentication mode of the packets sent on the interface to plain text mode; the "**no ip vrrp authentication mode**" command restores the default VRRP authentication mode.

Parameter: text means the VRRP authentication mode is plain text mode.

Command mode: Interface Mode

Default: There is no authentication by default.

Usage Guide: This command is used to avoid the interference of non-group members. All

the routers in the same standby group should set to the same authentication mode.

Example: Set the VRRP authentication mode to plain text mode.

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip vrrp authentication mode text

17.2.2.7 vrrp authentication string

Command: ip vrrp authentication string <string>

no ip vrrp authentication string

Function: Set the authentication string of the VRRP packets sent on the interface; the "**no ip vrrp authentication string**" command restores the default authentication string.

Parameter: <*string*> is the authentication string.

Command mode: Interface Mode

Default: There is no authentication string by default.

Usage Guide: This command is used to avoid the interference of non-group members. If all the routers in the same standby group are set to the plain text authentication mode, they have to use the same authentication string.

Example: Set the authentication string to public

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip vrrp authentication string public

17.2.2.8 preempt

Command: preempt-mode{true| false}

Function: Configure the VRRP preempt mode.

Command mode: VRRP Mode

Default: The preempt mode is enable by default.

Usage Guide: If users want to configure the router (or the layer3 switch) with high priority to preempt the master router, this feature should be enabled.

Example: Disable the preempt mode.

Switch(Config-Router-Vrrp)# preempt-mode false

17.2.2.9 priority

Command: priority <*value*>

no priority

Function: Configure VRRP priority; the "**no priority**" command restores to its default value 100. IP Owner's VRRP priority is always 255.

Parameter: <*value*> is the VRRP priority, valid range is 1 to 255.

Command mode: VRRP Mode

Default: The VRRP priority for the backup routers (or the layer 3 switches) is 100 by default, whereas the VRRP priority for the master router (or the layer 3 switch) is 255 by default.

Usage Guide: The priority of the routers in the VRRP backup group is used to elect the master router. When the router is set to the master virtual IP address, the priority is 255 which can't be changed. During the election, when two or more then two routers have the same VRRP priority, the router with the greatest IP address of the VLAN interface is elected as the master router.

Example: Set VRRP priority to 150

Switch(Config-Router-Vrrp)# priority 150

17.2.2.10 advertisement-interval

Command: advertisement-interval <*adver_interva*l>

no advertisement-interval

Function: Configure VRRP timer value; the "**no advertisement-interval**" command restores the default setting.

Parameter: <*adver_interva*> is the interval of sending VRRP message in seconds, valid range is 1 to 10.

Command mode: VRRP Mode

Default: <*adver_interva*> is 1 second by default.

Usage Guide: The master router in the VRRP standby group sends regularly the VRRP messages to inform the group members that it is working properly. This interval of sending VRRP messages is *adver_interval*. If the backup routers don't receive the VRRP messages for a certain period of time (*master_down_interval*), they consider that the master router is down. The backup routers will elect the new master router to forward the traffic.

Users can modify the interval of sending the VRRP messages. The routers in the same VRRP standby group should be set to the same value. For the backup routers, the value of *master_down_interval* should be three times of that of *adver_interval*. If the network traffic is significant or if the VRRP routers have different values for the timer, the *master_down_interval* may be overtime and it triggers the election of the new master router. In order to avoid this situation,

users can set greater *adver_interval* value or set greater preempt delay time.

Example: Set VRRP timer to 3 seconds

Switch(Config-Router-Vrrp)# advertisement-interval 3

17.2.2.11 circuit-failover

Command: circuit-failover <*ifname*> <*value_reduced*>

no circuit-failover

Function: Configure the VRRP monitored interface.

Parameter: < *ifname* > is the name of the monitored interface

<*value_reduced*> is reduced value of the VRRP priority, valid range is 1 to 253.

Command mode: VRRP Mode

Usage Guide: This is an expanded feature of the VRRP backup to ensure the successful new master router election. When the master router is down and the VRRP priority of the backup interfaces is lower than that of the failed master interface, the new master router election could fail. The VRRP monitored interface can solve this problem. When the monitored interface is down, the VRRP priority of the monitored interface is reduced. This mechanism avoids the unsuccessful new master router election.

Example: Set the VRRP monitored interface to vlan2 and the VRRP priority is reduced by 10.

Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10

17.2.3 Typical VRRP Application

Scenario:

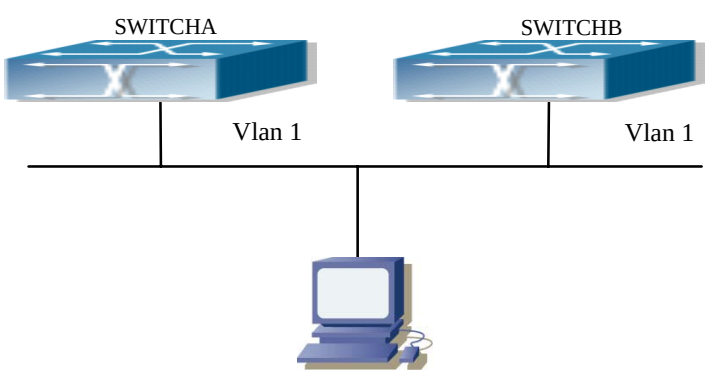


Fig 17-1 Typical VRRP Application Topology

SWITCHA and SWITCHB are layer 3 LAN switches in the same standby group. Set SWITCHA to master switch.

The configuration steps are listed below:

SWITCHA:

SwitchA(config)#interface vlan 1

SwitchA (Config-If-Vlan1)# ip address 10.1.1.5 255.255.255.0

SwitchA (Config-If-Vlan1)#exit

SwitchA (config)#router vrrp 1

SwitchA(Config-Router-Vrrp)# virtual-ip 10.1.1.5 master

SwitchA(Config-Router-Vrrp)# interface vlan 1

SwitchA(Config-Router-Vrrp)# enable

SWITCHB:

SwitchB(config)#interface vlan 1

SwitchB (Config-if-Vlan1)# ip address 10.1.1.7 255.255.255.0

SwitchB (Config-if-Vlan1)#exit

SwitchB(config)#router vrrp 1

SwitchB (Config-Router-Vrrp)# virtual-ip 10.1.1.5 backup

SwitchB(Config-Router-Vrrp)# interface vlan 1

SwitchB(Config-Router-Vrrp)# enable

17.2.4 VRRP Troubleshooting Help

17.2.4.1 Monitor and Debug Commands

17.2.4.1.1 show vrrp

Command: show vrrp [**<*vrid*>**]

Function: Display the state and the configuration of the standby group

Command mode: Any Mode

Example:

Switch# show vrrp

VrId <1>

State is Initialize

Virtual IP is 10.1.20.10 (Not IP owner)

Interface is Vlan2

Priority is 100

Advertisement interval is 1 sec

Preempt mode is TRUE

VrId <10>

State is Initialize

Virtual IP is 10.1.10.1 (IP owner)

Interface is Vlan1

Configured priority is 255, Current priority is 255

Advertisement interval is 1 sec

Preempt mode is TRUE

Circuit failover interface Vlan1, Priority Delta 10, Status UP

Item	Explanation
State	State
Virtual IP	Virtual IP address
Interface	Interface name
priority	priority
Advertisement interval	timer
Preempt	Preempt mode
Circuit failover interface	Monitored interface information

17.2.4.1.2 debug vrrp

Command: debug vrrp [**all | event | packet** [**recv| send**]]

no debug vrrp [**all | event | packet** [**recv| send**]]

Function: Display the state changes and messages sent and received for the standby group; the "**no debug vrrp [all | event | packet [recv| send]]**" command stops displaying debug information.

Command mode: Admin Mode

Default: Debug information is not displayed by default.

Example:

Switch#debug vrrp

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

17.2.4.2 VRRP Troubleshooting Help

VRRP may not work properly due to bad physical connection or wrong configuration. Users can troubleshoot the problems by following the guide below:

- ✧ Make sure the physical connection is good
- ✧ Use “show interfaces status” command to make sure the interface and link protocol are up
- ✧ Make sure VRRP is enabled on the interface
- ✧ Examine the routers (or layer 3 switches) in the same standby group are configured for the same authentication
- ✧ Examine the routers (or layer 3 switches) in the same standby group are configured for the same timer;
- ✧ Examine the virtual IP address and the interface IP addresses are in the same subnet.
- ✧ If the problems are still not solved. User can use “debug vrrp” command, copy debug information for 3 minutes, and send this information to Accton Technical Support Center.

Chapter 18 Cluster Network Management

18.1 Introduction to cluster network management

Cluster network management is an in-band configuration management. Unlike CLI, SNMP and Web Config which implement a direct management of the target switches through a management workstation, cluster network management implements a direct management of the target switches (member switches) through an intermediate switch (commander switch). A commander switch can manage multiple member switches. As soon as a Public IP address is configured in the commander switch, all the member switches which are configured with private IP addresses can be managed remotely. This feature economizes public IP addresses which are short of supply. Cluster network management can dynamically discover cluster feature enabled switches (candidate switches). Network managers can statically or dynamically add the candidate switches to the cluster which is already established. Accordingly, they can configure and manage the member switches through the commander switch. When the member switches are distributed in various physical locations (such as on the different floors of the same building), cluster network management has obvious advantages. Moreover, cluster network management is an in-band management. The commander switch can communicate with member switches with existing network. There is no need to build a specific network for network management.

Cluster network management has the following features:

- Save IP addresses
- Simplify configuration tasks
- Indifference to network protocol and network length limitation
- Auto detect and auto establishment
- With factory default settings, the switches can be managed by cluster network management
- The commander switch can upgrade and configure any member switches in the cluster

18.2 Basic Cluster Network Management Configuration

18.2.1 Cluster Network Management Configuration Sequence

Enable or disable cluster function

Create cluster

Create or delete cluster

Configure private IP address pool for member switches of the cluster

Add or remove a member switch

Configure attributes of the cluster in the commander switch

1) Enable or disable joining the cluster automatically
2) Set holdtime of heartbeat of the cluster
3) Set interval of sending heartbeat packets among the switches of the cluster
4) Clear the list of candidate switches discovered by the commander switch

Configure attributes of the cluster in the candidate switch

1) Set interval of sending cluster registration packet

Remote cluster network management

1) Remote configuration management
2) Reboot member switch
3) Remotely upgrade member switch

1. Enable or disable cluster

Command	Explanation
Global Mode	
cluster run **no cluster run**	Enable or disable cluster function in the switch

2. Create a cluster

Command	Explanation
Global Mode	
cluster commander <*cluster-name*> ***[vlan<vlan-id>]*** **no cluster commander**	Create or delete a cluster
cluster ip-pool<*commander-ip*> **no cluster ip-pool**	Configure private IP address pool for member switches of the cluster
cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>] }[password <*pass*>] **no cluster member < *mem-id* >**	Add or remove a member switch

3. Configure attributes of the cluster in the commander switch

Command	Explanation
Global Mode	
cluster auto-add enable **no cluster auto-add enable**	Enable or disable adding newly discovered candidate switch to the cluster
cluster holdtime < second> **no cluster holdtime**	Set holdtime of heartbeat of the cluster
cluster heartbeat <*interval*> **no cluster heartbeat**	Set interval of sending heartbeat packets among the switches of the cluster
clear cluster candidate table	Clear the list of candidate switches discovered by the commander switch

4. Configure attributes of the cluster in the candidate switch

Command	Explanation
Global Mode	
cluster register timer <*timer-value*> **no cluster register timer**	Set interval of sending cluster registration packet

5. Remote cluster network management

Command	Explanation
Admin Mode	
rcommand member <mem-id>	In the commander switch, this command is used to configure and manage member switches.
rcommand commander	In the member switch, this command is used to configure the member switch itself.
cluster reset member<mem-id>	In the commander switch, this command is used to reset the member switch.
cluster update member <*mem-id*> <*src-url*> <*dst-url*> [ascii | binary]	In the commander switch, this command is used to remotely upgrade the member switch.

18.2.2 Cluster Configuration Commands

18.2.2.1 cluster run

Command: cluster run

no cluster run

Function: Enable cluster function; the "**no cluster run**" command disables cluster function.

Command mode: Global Mode

Default: Cluster function is disabled by default.

Usage Guide: This command enables cluster function. Cluster function has to be enabled before implementing any other cluster commands. The "**no cluster run**" disables cluster function.

Example: Disable cluster function in the local switch.

Switch (Config)#no cluster run

18.2.2.2 cluster register timer

Command: cluster register timer<time-value>

no cluster register timer

Function: Sets interval of sending cluster registration packet; the "**no cluster register timer**" command restores the default setting.

Parameter: ***<timer-value>*** is interval of sending cluster registration packet in seconds, valid range is 30 to 65535.

Command mode: Global Mode

Default: Cluster register timer is 60 seconds by default.

Example: Set the interval of sending cluster registration packet to 80 seconds.

Switch(Config)#cluster register timer 80

18.2.2.3 cluster ip-pool

Command: cluster ip-pool <*commander-ip*>

no cluster ip-pool

Function: Configure private IP address pool for member switches of the cluster.

Parameter: ***<commander-ip>*** is the IP address of the commander switch in dotted decimal format. The value of the last byte in IP address is lower than (255-200).

Command mode: Global Mode

Default: There is no private IP address pool by default.

Usage Guide: Before creating the cluster, users have to set the private IP address pool in the commander switch. The cluster can't be created if the private IP address pool is not set. When candidate switches join the cluster, the commander switch assigns a private IP address for each member switch. These IP addresses are used to communicate between the commander switch and the member switches. This command can be only used in a non-member switch. As soon as the cluster is created, the users can't modify the IP address pool. The "no cluster ip-pool" command clears the address pool and there is no default setting to be restored.

Example: Set the private IP address pool for the member switches to 192.168.1.64

Switch(config)#cluster ip-pool 192.168.1.64

18.2.2.4 cluster commander

Command: cluster commander <*cluster-name*> [vlan <*vlan-id*>]

no cluster commander

Function: Enables a commander switch, create a cluster, or modify a cluster's name; the "**no cluster commander**" command deletes the cluster.

Parameter: <*cluster-name*> is the cluster's name; **<*vlan-id*>** is the VLAN of the Layer 3 device which the cluster belongs to. If it is omitted, the cluster belongs to VLAN1.

Command mode: Global Mode

Default: There is no cluster by default.

Usage Guide: This command sets the switch as a commander switch and creates a cluster. Before executing this command, users must configure a private IP address pool. If users executes this command again, the cluster's name will be changed and this information is distributed to the member switches. If users execute this command in a member switch, an error will be displayed. If users execute this command again with a new vlan id, the new vlan id is invalid.

Note: On layer3 interface that be configured cluster commander command, avoid configure RIP,OSPF routing protocol, otherwise, those routing protocols will not work.

Example: Set the switch as a commander switch. The cluster's name is admin and the vlan-id is vlan

Switch(config)#cluster commander admin vlan 2

18.2.2.5 cluster member

Command: cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>]} [password <*pass*>]

no cluster member < *mem-id* >

Function: Add a candidate switch to the cluster in the commander switch; the "**no cluster member < mem-id >**" command deletes a member switch from the cluster.

Parameter: <*mem-id*> is the member ID, valid range is 1 to 23; **<*cand-sn*>** is the sequence number of the switch in the candidate switch list, valid range is 0 to 127. Users can use ";" or "-" to specify multiple numbers or successive numbers; **<*mac-add*>** is the MAC address of the member switch in the format of XX-XX-XX-XX-XX-XX; **<*pass*>** is the privileged password of the member switch.

Command mode: Global Mode

Usage Guide: When this command is executed in the commander switch, the switch with **<*mac-add*>** or **<*cand-sn*>** will be added to the cluster which the commander switch belongs to. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, add the candidate switch which has the sequence number as 17 and password as mypassword to the cluster.

Switch(config)#cluster member candidate-sn 17 password mypassword

18.2.2.6 cluster auto-add

Command: cluster auto-add enable

no cluster auto-add enable

Function: When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the "**no cluster auto-add enable**" command disables this function.

Command mode: Global Mode

Default: This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.

Usage Guide: When this command is executed in the commander switch and the commander switch receives the cluster registration packets sent by the new switch, the commander switch adds the candidate switch to the cluster. If this command is executed in a non-commander switch, an error will be displayed.

Example: Enable the auto adding function in the commander switch.

Switch(config)#cluster auto-add enable

18.2.2.7 rcommand member

Command: rcommand member <*mem-id*>

Function: In the commander switch, this command is used to remotely manage the member switches in the cluster.

Parameter: <*mem-id*> is the cluster ID of the member switch, valid rang is 1 to 23.

Command mode: Admin Mode

Usage Guide: Enter the Admin Mode of the member switch and configure the member switch remotely. Use "**exit**" to quit the configuration interface of the member switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, enter the configuration interface of the member switch with mem-id 15.

Switch#rcommand member 15

18.2.2.8 rcommand commander

Command: rcommand commander

Function: In the member switch, use this command to configure the commander switch.

Command mode: Admin Mode

Usage Guide: This command is used to configure the commander switch remotely. Users have to telnet the commander switch by passing the authentication. The command "**exit**" is used to quit the configuration interface of the commander switch. If this command is executed in the commander switch, an error will be displayed.

Example: In the member switch, enter the configuration interface of the commander switch.

Switch#rcommand commander

18.2.2.9 cluster reset member

Command: cluster reset member <*mem-id*>

Function: In the commander switch, this command can be used to reset the member switch.

Parameter: <*mem-id*> is the cluster ID of the member switch, valid rang is 1 to 23.

Command mode: Admin Mode

Usage Guide: In the commander switch, users can use this command to reset a member switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, reset the member switch 16.

Switch#cluster reset member 16

18.2.2.10 cluster update member

Command: cluster update member <*mem-id*> <*src-url*> <*dst-url*> [ascii | binary]

Function: In the commander switch, this command is used to remotely upgrade the member switch.

Parameter: <*mem-id*> is the cluster ID of the member switch, valid rang is 1 to 23; **<*src-url*>** is the source path of the file which need to be copied; **<*dst-url*>** is the destination path of the file which need to be copied; **ascii** means that the file is transmitted in ASCII format; **binary** means that the file is transmitted in binary. When **<*src-url*>** is a FTP address, its format is like: ftp: //<*username*>: <*password*>@<*ipadress*>/<*filename*>. <*username*> is the FTP user name, <*password*> is the FTP password, <*ipadress*> is the IP address of the FTP server and <*filename*> is the file name. When **<*src-url*>** is a TFTP address, its format is like: tftp: //<*ipadress*>/<*filename*>. <*ipadress*> is the IP address of the TFTP server and <*filename*> is the file name.

The special keywords of filename:

Keyword	Source address or destination address
startup-config	Startup configuration file
nos.img	System file
boot.rom	System startup file

Command mode: Admin Mode

Usage Guide: The commander switch sends the remote upgrade command to the member switch. The member switch is upgraded and reset. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch sends the remote upgrade command to the member switch which has mem-id as 10, src-url as ftp: //admin: admin@192.168.1.1/nos.img and dst-url as nos.img

Switch#cluster update member 10 192.168.1.2 ftp: //admin: admin@192.168.1.1/nos.img nos.img

18.2.2.11 cluster holdtime

Command: cluster holdtime < *second*>

no cluster holdtime

Function: In the commander switch, set holdtime of heartbeat of the cluster; the "**no cluster holdtime**" command restores the default setting.

Parameter: <*second*> is the holdtime of heartbeat of the cluster, valid range is 20 to 65535. The holdtime of heartbeat means the maximum valid time of heartbeat packets. When the heartbeat packets are received again, the holdtime is reset. If no heartbeat packets are received in the holdtime, the cluster is invalid.

Command mode: Global Mode

Default: The holdtime of heartbeat is 80 seconds by default.

Usage Guide: In the commander switch, this command is used to set the holdtime of heartbeat. And this information is distributed to all the member switches. If this command is executed in a non-commander switch and the value is less than the current holdtime, the setting is invalid and an error is displayed.

Example: Set holdtime of heartbeat of the cluster to 100 seconds

Switch(config)#cluster holdtime 100

18.2.2.12 cluster heartbeat

Command: cluster heartbeat <*interval*>

no cluster heartbeat

Function: In the commander switch, set interval of sending heartbeat packets among the switches of the cluster; the "**no cluster heartbeat**" command restores the default setting.

Parameter: ***<interval>*** is the interval of heartbeat of the cluster, valid range is 1 to 65535.

Command mode: The interval of heartbeat is 8 seconds by default.

Default: Global Mode

Usage Guide: In the commander switch, this command is used to set the interval of heartbeat. And this information is distributed to all the member switches. If this command is executed in a non-commander switch and the value is more than the current holdtime, the setting is invalid and an error is displayed.

Example: Set the interval of sending heartbeat packets of the cluster to 10 seconds.

Switch(config)#cluster heartbeat 10

18.2.2.13 clear cluster candidate-table

Command: clear cluster candidate-table

Function: Clear the list of candidate switches discovered by the commander switch.

Command mode: Admin Mode

Usage Guide: In the commander switch, this command is used to clear the list of candidate switches discovered by the commander switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: Clear the list of candidate switches discovered by the commander switch

Switch#clear cluster candidate-table